ProCurve
Networking by HP

8212zl
6200yl
5400zl
3500yl

Command Line Interface Reference Guide

ProCurve Switches

K.13.XX

www.procurve.com

hp
invent

ProCurve Networking
HP Innovation

Command Line Interface Reference Guide

Switch 8212zl
Series 6200yl Switch
Series 5400zl Switch
Series 3500yl Switch

Software Release K.13.XX, Software Version as of January 2008

invent

Hewlett-Packard Company

Publication Number

5992-3063

March 2008

Copyright

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Trademark Credits

Contents

Part I. Introduction

Introduction

CONVENTIONS

Abstract

This guide uses the following conventions for command syntax and displayed information.

Command Syntax Statements

Syntax:

```
aaa port-access authenticator PORT-LIST [ control < authorized | auto |
unauthorized >]
```

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces (< >) enclose required elements.
- Square brackets or braces within square brackets ([< >]) indicate a required element within an optional choice.
- All caps indicate variables for which you must supply a value when executing the command. For example, in this command syntax, you must provide one or more port numbers:

  Syntax:

  ```
  aaa port-access authenticator PORT-LIST
  ```

Command Prompts

In the default configuration the Series 8212zl switches, for example, display the following CLI prompt:

- ProCurve Switch 8212zl#

To simplify recognition, this guide uses ProCurve or HPswitch to represent command prompts for all models. For example:

```
ProCurve#
```

```
HPswitch#
```

(You can use the hostname command to change the text in the CLI prompt.)

Example Commands

Example commands and their output appear in the Courier type face. For example:

```
ProCurve(config)# clear public-key
ProCurve(config)# show ip client-public-key
show_client_public_key: cannot stat keyfile
```

Port Numbering Conventions

ProCurve chassis switches designate individual ports with a letter/number combination to show the slot in which the port is found and the sequential number the port has in that slot (A1, A2, B1, B2, etc.)

GETTING DOCUMENTATION FROM THE WEB

You need the Adobe® Acrobat® Reader to view, print, and/or copy ProCurve Networking product documentation.

1. Go to the ProCurve Networking Web site at **www.procurve.com** [http://www.procurve.com.]
2. Click on Technical support, then Product manuals(all).
3. Click on the name of the product for which you want documentation.
4. On the resulting Web page, double-click on a document you want to view or download.

CLI ONLINE HELP

To access the online help, type the command, followed by a space, then press the [Tab] key.

List Available Commands

Type “?” to list available commands. Typing the ? symbol lists the commands you can execute at the current privilege level.

Use [Tab] to search for or complete a command word. You can use [Tab] to help you find CLI commands or to quickly complete the current word in a command. To do so, type one or more consecutive characters in a command and then press [Tab] (with no spaces allowed). Pressing [Tab] after a completed command word lists the further options for that command.

Options Available in Current Context

You can use the CLI to remind you of the options available for a command by entering command keywords followed by ?.

Displaying Command-List Help

Syntax: help

Displays a listing of command help summaries for all commands available at the current privilege level. That is, at the Operator level, executing help displays the help summaries only for Operator-Level commands. At the Manager level, executing help displays the help summaries for both the Operator and Manager levels, and so on.

Displaying Help for an Individual Command

Syntax: COMMAND-STRING help

This option displays help for any command available at the current context level.

RELATED PUBLICATIONS

The following documents (available on the ProCurve website) provide additional information on the CLI commands.

Software Release Notes

Release notes provide information on new software updates:

- New features and how to configure and use them
- Software management, including downloading software to the switch
- Software fixes addressed in current and previous releases

Product Notes and Software Update Information

The printed Read Me First shipped with your switch provides product notes and other information.

Installation and Getting Started Guide

Use the Installation and Getting Started Guide shipped with your switch to prepare for and perform the physical installation. This guide also steps you through connecting the switch to your network and assigning IP addressing, and describes the LED indications for correct operation and trouble analysis. A PDF version of this guide is also provided on the Product Documentation CD-ROM shipped with the switch. And you can download a copy from the ProCurve website.

Management and Configuration Guide

Use the Management and Configuration Guide for information on:

- Using the command line (CLI), Menu interface, and web browser interface
- Memory and configuration operation
- IP addressing
- Time protocols
- Port configuration, trunking, traffic control, and PoE operation
- Redundancy
- SNMP, LLDP, and other network management topics
- File transfers, switch monitoring, troubleshooting, and MAC address management
- Resource management
- Scalability

Access Security Guide

Use the Access Security Guide to learn how to use and configure the following access security features available in the switch:

- Local username and password security
- Web-based and MAC-based authentication
- Virus-throttling
- RADIUS and TACACS+ authentication
- SSH (Secure Shell) and SSL (Secure Socket Layer) operation
- 802.1X access control
- Port security operation with MAC-based control
- Authorized IP Manager security

- Access Control Lists (ACLs)
- KMS (Key Management System)

Advanced Traffic Management Guide

Use the Advanced Traffic Management Guide for information on:

- VLANs: Static port-based and protocol VLANs, and dynamic GVRP VLANs
- Spanning-Tree: 802.1D (STP), 802.1w (RSTP), and 802.1s (MSTP)
- Meshing
- Quality-of-Service (QoS)
- QinQ

Multicast and Routing Guide

Use the Multicast and Routing Guide for information on:

- IGMP
- PIM (SM and DM)
- IP routing
- VRRP

IPv6 Configuration Guide

Use the IPv6 Configuration Guide for information on:

- Migrating to IPv6
- IPv6 Configuration and Management
- IPv6 Security
- IPv6 Troubleshooting
- IPv6 Scalability

HOW TO NAVIGATE THIS GUIDE

The commands and page numbers in this guide are hyperlinked in blue to allow you to easily navigate to the desired command detail. Hyperlinked areas are:

- Overview: Related commands section
- Command Structure
- Command Details summary listing
- Next Available Options within individual command options and parameters
- Page numbers displayed with commands

When the hand cursor is positioned over a blue hyperlinked area, the hand displays a pointing finger. Left-click once to go the the indicated command. Additionally, the Command Details section lists the commands in alphabetical order.

Navigating Printed Copy

If you are using a printed copy of this guide, use the page numbers displayed at the end of a command, option, or parameter to go to the desired command detail.

Traversing the Command Structure

The commands shown in the Command Structure section of a chapter mimic the command organization of the switch. For example, if you select the command "aaa", one of the next command options is "accounting". The next available option under accounting is "commands". The Command

Structure provides a high-level view of all the command options and parameters for that command. Each of these is hyperlinked to take you to the details about that option or parameter.

Part II. Commands

aaa

OVERVIEW

Category:	802.1X, Accounting, Switch Security
Primary context:	config
Related Commands	**show authentication (page 454)** **show port-access (page 495)** **show accounting (page 452)** **show radius (page 500)** **show tacacs (page 513)** **radius-server (page 393)** **tacacs-server (page 585)**

```
Usage: aaa <...>

Description: Configure the switch Authentication, Authorization, and Accounting
             features. Use 'aaa ?' command to see a list of all possible
             configuration options.
```

COMMAND STRUCTURE

- [no] aaa **accounting** -- Configure accounting parameters on the switch **(p. 26)**
  - **commands** -- Configure 'commands' type of accounting **(p. 32)**
    - **mode < stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 40)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 39)**
  - **exec** -- Configure 'exec' type of accounting **(p. 34)**
    - **mode < start-stop | stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 40)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 39)**
  - **network** -- Configure 'network' type of accounting **(p. 41)**
    - **mode < start-stop | stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 40)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 39)**
  - **suppress** -- Do not generate accounting records for a specific type of user. **(p. 51)**
    - **null-username** -- Do not generate accounting records for users with a null-username. **(p. 41)**
  - **system** -- Configure 'system' type of accounting **(p. 51)**
    - **mode < start-stop | stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 40)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 39)**
  - **update** -- Configure update accounting records mechanism **(p. 53)**
    - **periodic < 1 to 525600 >** -- Configure update accounting records mechanism **(p. 41)**
- [no] aaa **authentication** -- Configure authentication parameters on the switch **(p. 27)**
  - **console** -- Configure authentication mechanism used to control access to the switch console **(p. 32)**
    - **enable** -- Configure access to the privileged mode commands. **(p. 33)**
      - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 43)**
        - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
    - **login** -- Configure login access to the switch. **(p. 35)**

    - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 43)**
      - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
- **login** -- Specify that switch respects the authentication server's privilege level **(p. 35)**
  - **privilege-mode** -- Specify that switch respects the authentication server's privilege level **(p. 46)**
- **mac-based** -- Configure authentication mechanism used to control mac-based port access to the switch **(p. 36)**
  - **primary < chap-radius | peap-mschapv2 >** -- Specify the primary authentication method for access control. **(p. 43)**
    - **secondary < none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
- **num-attempts < 1 to 10 >** -- Specify the maximum number of login attempts allowed **(p. 41)**
- **port-access** -- Configure authentication mechanism used to control access to the network **(p. 42)**
  - **primary < local | eap-radius | chap-radius >** -- Specify the primary authentication method for access control. **(p. 43)**
    - **secondary < none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
- **ssh** -- Configure authentication mechanism used to control SSH access to the switch **(p. 49)**
  - **enable** -- Configure access to the privileged mode commands. **(p. 33)**
    - **primary < local | tacacs | radius | ... >** -- Specify the primary authentication method for access control. **(p. 43)**
      - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
  - **login** -- Configure login access to the switch. **(p. 35)**
    - **primary < local | tacacs | radius | ... >** -- Specify the primary authentication method for access control. **(p. 43)**
      - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
- **telnet** -- Configure authentication mechanism used to control telnet access to the switch **(p. 52)**
  - **enable** -- Configure access to the privileged mode commands. **(p. 33)**
    - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 43)**
      - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
  - **login** -- Configure login access to the switch. **(p. 35)**
    - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 43)**
      - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
- **web** -- Configure authentication mechanism used to control web access to the switch **(p. 54)**
  - **enable** -- Configure access to the privileged mode commands. **(p. 33)**
    - **primary < local | radius >** -- Specify the primary authentication method for access control. **(p. 43)**
      - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
  - **login** -- Configure login access to the switch. **(p. 35)**
    - **primary < local | radius >** -- Specify the primary authentication method for access control. **(p. 43)**

            - **secondary < local | none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
    - **web-based** -- Configure authentication mechanism used to control web-based port access to the switch **(p. 54)**
        - **primary < chap-radius | peap-mschapv2 >** -- Specify the primary authentication method for access control. **(p. 43)**
            - **secondary < none | authorized >** -- Specify the backup authentication method for access control. **(p. 47)**
- [no] aaa **authorization** -- Configure authorization parameters on the switch **(p. 30)**
    - **commands** -- Configure exec (shell) commands authorization. **(p. 32)**
        - **primary_method < radius | none >** -- **(p. 46)**
- [no] aaa **port-access** -- Configure 802.1X port access. **(p. 42)**
    - **authenticator** -- Configure 802.1X authentication. **(p. 28)**
        - **active** -- Activate/deactivate 802.1X authenticator. **(p. 27)**
        - **PORT-LIST** -- Manage 802.1X on the device port(s). ([ethernet] PORT-LIST) **(p. 42)**
            - **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default). **(p. 30)**
                - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 53)**
            - **clear-statistics** -- Clear the authenticator statistics. **(p. 31)**
            - **client-limit** -- Set the maximum number of clients to allow on the port. **(p. 31)**
                - **NUMBER-OF-CLIENTS < 1 to 32 >** -- Set the maximum number of clients to allow on the port. (NUMBER) **(p. 41)**
            - **control < authorized | auto | unauthorized >** -- Set the authenticator to Force Authorized, Force Unauthorized or Auto state (default Auto). (NUMBER) **(p. 32)**
            - **initialize** -- Reinitialize the authenticator state machine. **(p. 35)**
            - **logoff-period < 1 to 999999999 >** -- Set period of time after which a client will be considered removed from the port for a lack of activity. (NUMBER) **(p. 36)**
            - **max-requests < 1 to 10 >** -- Set maximum number of times the switch retransmits authentication requests (default 2). (NUMBER) **(p. 39)**
            - **quiet-period < 0 to 65535 >** -- Set the period of time the switch does not try to acquire a supplicant (default 60 sec.). (NUMBER) **(p. 46)**
            - **reauthenticate** -- Force re-authentication to happen. **(p. 47)**
            - **reauth-period < 0 to 9999999 >** -- Set the re-authentication timeout (in seconds, default 0); set to '0' to disable re-authentication. (NUMBER) **(p. 47)**
            - **server-timeout < 1 to 300 >** -- Set the authentication server response timeout (default 30sec.). (NUMBER) **(p. 49)**
            - **supplicant-timeout < 1 to 300 >** -- Set the supplicant response timeout on an EAP request (default 30 sec.). (NUMBER) **(p. 51)**
            - **tx-period < 1 to 65535 >** -- Set the period of time the switch waits until retransmission of EAPOL PDU (default 30 sec.). (NUMBER) **(p. 52)**
            - **unauth-period < 0 to 255 >** -- Set period of time the switch waits for authentication before moving the port to the VLAN for unauthenticated clients. (NUMBER) **(p. 52)**
            - **unauth-vid** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default). **(p. 52)**
                - **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default). (VLAN-ID) **(p. 53)**
    - **gvrp-vlans** -- Enable/disable the use of RADIUS-assigned dynamic (GVRP) VLANs **(p. 34)**
    - **mac-based** -- Configure MAC address based network authentication on the device or the device's port(s) **(p. 36)**
        - **addr-format < no-delimiter | single-dash | multi-dash | ... >** -- Set the MAC address format to be used in the RADIUS request message (default no-delimiter). **(p. 27)**

- **mac-list1** -- Manage MAC address based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 38)**
  - **addr-limit < 1 to 32 >** -- Set the port's maximum number of authenticated MAC addresses (default 1). (NUMBER) **(p. 27)**
  - **addr-moves** -- Set whether the MAC can move between ports (default disabled - no moves). **(p. 27)**
  - **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default). **(p. 30)**
    - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 53)**
  - **logoff-period < 1 to 9999999 >** -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 36)**
  - **max-requests < 1 to 10 >** -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 39)**
  - **quiet-period < 1 to 65535 >** -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 46)**
  - **reauthenticate** -- Force re-authentication to happen. **(p. 47)**
  - **reauth-period < 0 to 9999999 >** -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 47)**
  - **server-timeout < 1 to 300 >** -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 49)**
  - **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). **(p. 52)**
    - **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 53)**

- **PORT-LIST** -- Manage general port security features on the device port(s). ([ethernet] PORT-LIST) **(p. 42)**
  - **controlled-direction < both | in >** -- Configure how traffic is controlled on non-authenticated ports; in BOTH directions (ingress+egress) or IN only (ingress). (NUMBER) **(p. 33)**
- **supplicant** -- Manage 802.1X supplicant. ([ethernet] PORT-LIST) **(p. 50)**
  - **auth-timeout < 1 to 300 >** -- Set the challenge reception timeout (default 30sec.). (NUMBER) **(p. 30)**
  - **clear-statistics** -- Clear the supplicant statistics. **(p. 31)**
  - **held-period < 0 to 65535 >** -- Set the held period (default 60sec.). (NUMBER) **(p. 35)**
  - **identity** -- Set the identity(user name) to be used by the supplicant. (ASCII-STR) **(p. 35)**
    - **secret** -- **(p. 49)**
  - **initialize** -- Reinitialize the supplicant state machine. **(p. 35)**
  - **max-start < 1 to 10 >** -- Define the maximum number of attempts taken to start authentication (default 3). (NUMBER) **(p. 39)**
  - **secret** -- Trigger the command to ask user for a password for the supplicant to use. **(p. 49)**
  - **start-period < 1 to 300 >** -- Set a period of time between EAPOL-Start packet retransmission (default 30sec.). (NUMBER) **(p. 50)**
- **web-based** -- Configure web authentication based network authentication on the device or the device's port(s) **(p. 54)**
  - **dhcp-addr** -- Set the base address / mask for the temporary pool used by DHCP (base address default is 192.168.0.0, mask default is 24 - 255.255.255.0). (IP-ADDR/MASK-LENGTH) **(p. 33)**
  - **dhcp-lease < 5 to 25 >** -- Set the lease length of the IP address issued by DHCP (default 10). (NUMBER) **(p. 33)**
  - **web-list1** -- Manage web authentication based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 56)**
    - **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default). **(p. 30)**

  - **web-authvid** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 54)**
- **client-limit < 1 to 32 >** -- Set the port's maximum number of authenticated clients (default 1). (NUMBER) **(p. 31)**
- **client-moves** -- Set whether the client can move between ports (default disabled - no moves). **(p. 31)**
- **logoff-period < 1 to 9999999 >** -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 36)**
- **max-requests < 1 to 10 >** -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 39)**
- **max-retries < 1 to 10 >** -- Set number of times a client can enter their credentials before authentication is considered to have failed (default 3). (NUMBER) **(p. 39)**
- **quiet-period < 1 to 65535 >** -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 46)**
- **reauthenticate** -- Force re-authentication to happen. **(p. 47)**
- **reauth-period < 0 to 9999999 >** -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 47)**
- **redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length. **(p. 47)**
  - **web-redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length. (ASCII-STR) **(p. 57)**
- **server-timeout < 1 to 300 >** -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 49)**
- **ssl-login** -- Set whether to enable SSL login (https on port 443) (default disabled). **(p. 50)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). **(p. 52)**
  - **web-unauthvid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 57)**

EXAMPLES

Example: aaa

The following examples show access options, and the corresponding commands to configure them.

Authenticate console enable (Manager) access, using TACACS+ as the primary method and the switch's local database as the secondary method:

```
ProCurve(config)# aaa authentication console enable tacacs local
```

Authenticate Telnet login (Operator) access, using TACACS+ as the primary method and the switch's local database as the secondary method:

```
ProCurve(config)# aaa authentication Telnet login tacacs local
```

Authenticate Telnet login (Manager) access, using TACACS+ as the primary method and the switch's local database as the secondary method:

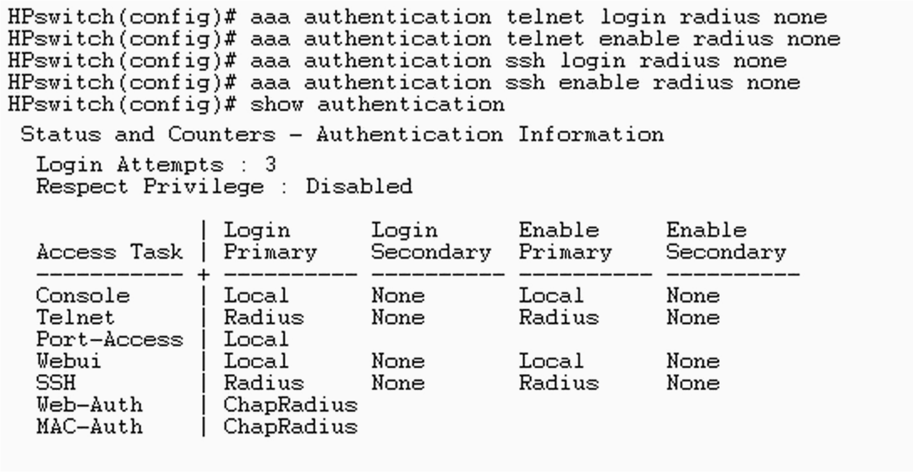
```
ProCurve(config)# aaa authentication telnet enable tacacs local
```

Deny access and terminate a session after two consecutive failures to provide the correct username and password:

```
ProCurve(config)# aaa authentication num-attempts 2
```

Example: aaa authentication

If you already configured local passwords on the switch, but want RADIUS to protect primary Telnet and SSH access without allowing a secondary Telnet or SSH access option (the switch's local passwords), type the following commands:



```
HPswitch(config)# aaa authentication telnet login radius none
HPswitch(config)# aaa authentication telnet enable radius none
HPswitch(config)# aaa authentication ssh login radius none
HPswitch(config)# aaa authentication ssh enable radius none
HPswitch(config)# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Radius     None       Radius     None
  Port-Access | Local
  Webui       | Local      None       Local      None
  SSH         | Radius     None       Radius     None
  Web-Auth    | ChapRadius
  MAC-Auth    | ChapRadius
```

Example: aaa authentication port-access eap-radius

Configure the switch for 802.1X authentication using an EAP-RADIUS server:

```
ProCurve(config)# aaa authentication port-access eap-radius
```

Example: aaa port-access authenticator

Configure ports A10 - A20 as 802.1X authenticator ports:

```
ProCurve(config)# aaa port-access authenticator a10-a20
```

Example: aaa port-access authenticator active

Activate 802.1X port-access on ports you have configured as authenticators:

```
ProCurve(config)# aaa port-access authenticator active
```

Example: aaa port-access authenticator auth-vid

Configure ports A10 - A20 to use VLAN 81 as the Authorized-Client VLAN:

```
ProCurve(config)# aaa port-access authenticator e a10-a20 auth-vid 81
```

Example: aaa port-access authenticator unauth-vid

Configure ports A10 - A20 to use VLAN 80 as the Unauthorized-Client VLAN:

```
ProCurve(config)# aaa port-access authenticator e a10-a20 unauth-vid 80
```

COMMAND DETAILS

accounting (p. 26)
active (p. 27)
addr-format (p. 27)
initialize (p. 35)
login (p. 35)
logoff-period (p. 36)
secondary (p. 47)
secret (p. 49)
server-timeout (p. 49)

accounting

- aaa accounting

```
Usage: [no] aaa accounting <exec|network|system|commands>
                           <start-stop|stop-only>
                           <radius>
       [no] aaa accounting update periodic <number>
       [no] aaa accounting suppress null-username

Description: Configure accounting parameters on the switch. The first form
             of the command can be used to specify a type of accounting,
             how accounting session will be started and ended, and the method
             used for accounting. The second form can be used to indicate of
             whether the send interim accounting records mechanism needs to be
             activated and how to issue an update of accounting records.
             The third form can be used to suppress accounting when an unknown
             user with no username accesses the switch
Parameters:
            o exec       - Provides information about user EXEC terminal
                           sessions (user shells) on the switch.
            o network    - Provides information about 8021x sessions.
            o system     - Provides information about all system-level events,
                           such as the system reboots or accounting turned
                           on/off.
            o commands   - Provides information about commands executed on the
                           switch.
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end of the
                           accounting session. Do not wait for acknowledgement.
            o stop-only  - Send a stop record accounting notice at the end of
                           the accounting session.Do not wait for
                           acknowledgement.
            o radius     - Use RADIUS as the accounting protocol
                           accounting information is available.
            o update periodic <number> - Send accounting update records at
```

```
                              regular intervals given by 'number' (in minutes).
               o suppress null-username - suppress accounting when a user with
                              no username accesses the switch
```

Next Available Options:

- **commands** -- Configure 'commands' type of accounting**(p. 32)**
- **exec** -- Configure 'exec' type of accounting**(p. 34)**
- **network** -- Configure 'network' type of accounting**(p. 41)**
- **suppress** -- Do not generate accounting records for a specific type of user. **(p. 51)**
- **system** -- Configure 'system' type of accounting**(p. 51)**
- **update** -- Configure update accounting records mechanism**(p. 53)**

active

- [no] aaa port-access authenticator active

```
Activate/deactivate 802.1X authenticator.
```

addr-format

- aaa port-access mac-based addr-format *< no-delimiter | single-dash | multi-dash | ... >*

```
Set the MAC address format to be used in the RADIUS request message (default
no-delimiter).
```

Supported Values:

- **no-delimiter** -- no delimiter format: aabbccddeeff.
- **single-dash** -- single dash format: aabbcc-ddeeff.
- **multi-dash** -- multi-dash format: aa-bb-cc-dd-ee-ff.
- **multi-colon** -- multi-colon format: aa:bb:cc:dd:ee:ff.
- **no-delimiter-uppercase** -- no delimiter, uppercase format: AABBCCDDEEFF.
- **single-dash-uppercase** -- single dash, uppercase format: AABBCC-DDEEFF.
- **multi-dash-uppercase** -- multi-dash, uppercase format: AA-BB-CC-DD-EE-FF.
- **multi-colon-uppercase** -- multi-colon, uppercase format: AA:BB:CC:DD:EE:FF.

addr-limit

- aaa port-access mac-based *[ETHERNET] PORT-LIST* addr-limit *< 1 to 32 >*

```
Set the port's maximum number of authenticated MAC addresses (default 1).
```

Range: < 1 to 32 >

addr-moves

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST* addr-moves

```
Set whether the MAC can move between ports (default disabled - no moves).
```

authentication

- aaa authentication

```
Usage: aaa authentication ...

Description: Configure authentication parameters on the switch.
             The command configures authentication mechanism used to
```

```
                control access the switch resources. Use 'aaa authentication ?'
                command to see a list of all possible configuration options.
```

Next Available Options:

- **console** -- Configure authentication mechanism used to control access to the switch console**(p. 32)**
- **telnet** -- Configure authentication mechanism used to control telnet access to the switch**(p. 52)**
- **web** -- Configure authentication mechanism used to control web access to the switch**(p. 54)**
- **ssh** -- Configure authentication mechanism used to control SSH access to the switch**(p. 49)**
- **port-access** -- Configure authentication mechanism used to control access to the network**(p. 42)**
- **web-based** -- Configure authentication mechanism used to control web-based port access to the switch**(p. 54)**
- **mac-based** -- Configure authentication mechanism used to control mac-based port access to the switch**(p. 36)**
- **num-attempts** < 1 to 10 > -- Specify the maximum number of login attempts allowed**(p. 41)**
- **login** -- Specify that switch respects the authentication server's privilege level**(p. 35)**

authenticator

- aaa port-access authenticator

```
Usage:  [no] aaa port-access authenticator active

        [no] aaa port-access authenticator [ethernet] PORT-LIST
        [control <authorized|auto|unauthorized> | quiet-period <0-65535> |
         tx-period <1-65535> | supplicant-timeout <1-300> |
         server-timeout <1-300> | max-requests <1-10> |
         reauth-period <0-9999999> | auth-vid VLAN-ID | unauth-vid VLAN-ID |
         unauth-period <0-255> | logoff-period <1-999999999> |
         client-limit [<1-32>] |
         initialize | reauthenticate | clear-statistics]

Description: Configure 802.1X (Port Based Network Access) authentication
             on the device or the device's port(s).

             The first form of the command activates or deactivates
             authentication on the device. By default, authentication is
             deactivated. 802.1X authentication does not run on the switch
             until you use this command to enable it.

             The second form of the command enables, disables, or
             configures authentication on the device's individual ports.

             While authentication is deactivated, access to the network
             is granted on all switch ports regardless of whether
             802.1X is enabled on the port.

             The 'no' keyword cannot be used with any of the optional
             parameters that follow PORT-LIST.

             802.1X must be enabled on a port before any of the following
             optional parameters can be configured on the port.

             o 'control' sets the authenticator to (Force) Authorized,
               (Force) Unauthorized or Auto state (default 'Auto').
```

```
  - Auto: Grants network access to a connected device that
          supports 802.1X authentication and provides valid
          credentials.
  - Authorized: Grants access to any devices connected to
          the port(s). In this case, the devices do not have
          to provide 802.1X credentials or support 802.1X
          authentication. (Also termed ''Force Authorized''.)
  - Unauthorized: In this state, the port blocks access to
          any connected device, regardless of whether the
          device provides the correct credentials and has
          802.1X support.

o 'quiet-period' sets the period of time during which the
  switch does not try to acquire a supplicant after a failed
  authentication attempt(default 60 seconds).

o 'tx-period' sets the period of time the switch waits to
  retransmit the next EAPOL PDU during an authentication
  session (default 30 seconds).

o 'server-timeout' sets the period of time after which the
  switch assumes that authentication has timed out
  (default 30 seconds).

o 'supp-timeout' sets the period of time after which the
  switch decides that a supplicant has not responded to an EAP
  request (default 30 seconds).

o 'max-requests' sets maximum number of times the switch
  retransmits a request to the backend authentication system
  (RADIUS server) before closing the current authentication
  session (default 2).

o 'reauth-period' sets the period of time after which connected
  clients must be re-authenticated. When the timeout
  is set to 0 the re-authentication is disabled (default 0
  seconds).

o 'auth-vid' configures the VLAN to which to move port after
  successful authentication. RADIUS server can override the
  value. Use 'no' form of the command to set this PVID to 0.
  If the PVID set to 0 no PVID changes occure unless RADIUS
  server requests. Changes take effect after client
  reauthentication. The default is 0.

o 'unauth-vid' configures the VLAN to which to move port if
  an unauthorized client has been connected on the port and
  there is no other client on the port. The switch will wait
  for the amount of time specified as the 'unauth-period'
  before the port will be moved to this VLAN. If the port PVID
  successfully set to the value configured, the port becomes
  unblocked and the client can communicate to other members
  of this VLAN. Use 'no' form of the command to set this PVID
  to 0. Changes take effect immediately. The default is 0.

o 'unauth-period' sets period of time the switch waits for
  authentication before assigning the 'unauth-vid' to the port
  if an unauthenticated client has been detected on this port.
  The default is 0 seconds.
```

```
o 'logoff-period' sets period of time after which a client will
  be considered removed from the port for a lack of activity.
  The default is 300 seconds.

o 'client-limit' sets the maximum number of clients to allow on
  the port. This includes ALL clients (authenticated and
  unauthenticated).
  NOTE: No more than 32 unique client MAC addresses can be
        authorized by both 802.1X and MAC/web-based
        authentication together on the same port.
  The 'no... client-limit' command allows unlimited number of
  clients on the port. Authenticator makes no distinction between
  clients and operates port as a single protocol entity with
  no specific MAC address filter on the port.
  The default is no client limit.

o 'initialize' re-initialize authentication on the specified
  ports. That is, 'initialize' blocks inbound and outbound
  traffic and restarts the authentication process on the
  specified ports that are configured with 'control auto' (see
  the 'control' parameter, described above) and actively
  operating as authenticators.

o 'reauthenticate' forces re-authentication (unless the
  authenticator is in 'HELD' state).

o 'clear-statistics' clears authenticator statistics
  counters.
```

Next Available Options:

- **PORT-LIST** -- Manage 802.1X on the device port(s). ([ethernet] PORT-LIST) **(p. 42)**
- **active** -- Activate/deactivate 802.1X authenticator.**(p. 27)**

authorization

- aaa authorization

```
Usage: [no] aaa authorization <commands> <radius>

Description: Configure authorization parameters on the switch.
```

Next Available Option:

- **commands** -- Configure exec (shell) commands authorization. **(p. 32)**

auth-timeout

- aaa port-access supplicant *[ETHERNET] PORT-LIST* auth-timeout *< 1 to 300 >*

```
Set the challenge reception timeout (default 30sec.).
```

Range: < 1 to 300 >

auth-vid

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST* auth-vid

```
Configures VLAN where to move port after successful authentication (not configured
by default).
```

Next Available Option:

- **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 53)**

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST* auth-vid

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

  Next Available Option:

  - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 53)**

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* auth-vid

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

  Next Available Option:

  - **web-authvid** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 54)**

clear-statistics

- aaa port-access authenticator *[ETHERNET] PORT-LIST* clear-statistics

  ```
  Clear the authenticator statistics.
  ```

- aaa port-access supplicant *[ETHERNET] PORT-LIST* clear-statistics

  ```
  Clear the supplicant statistics.
  ```

client-limit

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST* client-limit

  ```
  Set the maximum number of clients to allow on the port.
  ```

  Next Available Option:

  - **NUMBER-OF-CLIENTS** < 1 to 32 > -- Set the maximum number of clients to allow on the port. (NUMBER) **(p. 41)**

- aaa port-access web-based *[ETHERNET] PORT-LIST* client-limit *< 1 to 32 >*

  ```
  Set the port's maximum number of authenticated clients (default 1).
  ```

  Range: < 1 to 32 >

client-moves

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* client-moves

  ```
  Set whether the client can move between ports (default disabled - no moves).
  ```

commands

- [no] aaa accounting commands

```
Usage: [no] aaa accounting commands <stop-only> <radius>

Description: Configure 'commands' type of accounting.
Parameters:
            o stop-only - Send a record accounting notice after the execution
                          of command.
            o radius    - Use RADIUS as the accounting protocol.
```

Next Available Option:

- **mode** < stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 40)**

- [no] aaa authorization commands

```
Configure exec (shell) commands authorization.
```

Next Available Option:

- **primary_method** < radius | none > -- **(p. 46)**

console

- aaa authentication console

```
Usage: aaa authentication console <enable|login>
                                  <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control access
             to the switch console.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
                                 primary authentication method to get a list
                                 of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 33)**
- **login** -- Configure login access to the switch.**(p. 35)**

control

- aaa port-access authenticator *[ETHERNET] PORT-LIST* control < *authorized* | *auto* | *unauthorized* >

```
Set the authenticator to Force Authorized, Force
Unauthorized or Auto state (default Auto).
```

Supported Values:

- **authorized** -- Force authorized.
- **auto** -- Auto.
- **unauthorized** -- Force unauthorized.

controlled-direction

- aaa port-access *[ETHERNET] PORT-LIST* controlled-direction *< both | in >*

```
Configure how traffic is controlled on non-authenticated ports; in
BOTH directions (ingress+egress) or IN only (ingress).
```

Supported Values:

- **both** -- Exert control in both directions.
- **in** -- Exert control on incoming packets.

dhcp-addr

- aaa port-access web-based dhcp-addr *IP-ADDR/MASK-LENGTH*

```
Set the base address / mask for the temporary pool used by DHCP (base address default
 is 192.168.0.0, mask default is 24 - 255.255.255.0).
```

dhcp-lease

- aaa port-access web-based dhcp-lease *< 5 to 25 >*

```
Set the lease length of the IP address issued by DHCP (default 10).
```

Range: < 5 to 25 >

enable

- aaa authentication console enable

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication telnet enable

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication web enable

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication ssh enable

  ```
  Configure access to the privileged mode commands.
  ```

  Next Available Option:

  - **primary** < local | tacacs | radius | ... > -- Specify the primary authentication method for access control.**(p. 43)**

exec

- [no] aaa accounting exec

  ```
  Usage: [no] aaa accounting exec <start-stop|stop-only>
                                  <radius>

  Description: Configure 'exec' type of accounting.
  Parameters:
              o start-stop - Send a start record accounting notice at the
                             beginning and a stop record notice at the end
                             of the accounting session. Do not wait for
                             acknowledgement.
              o stop-only  - Send a stop record accounting notice at the end
                             of the accounting session.Do not wait for
                             acknowledgement.
              o radius     - Use RADIUS as the accounting protocol
  ```

  Next Available Option:

  - **mode** < start-stop | stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 40)**

gvrp-vlans

- [no] aaa port-access gvrp-vlans

  ```
  Usage:  [no] aaa port-access gvrp-vlans

  Description: Enables the use of dynamic VLANs (learned through GVRP) in the
  temporary untagged VLAN assigned by a RADIUS server on an authenticated port
  in an 802.1X, MAC, or Web authentication session.
  Enter the no form of this command to disable the use of GVRP-learned VLANs
  in an authentication session.

  Notes:
  1. If a port is assigned as a member of an untagged dynamic VLAN, the dynamic
     VLAN configuration must exist at the time of authentication and GVRP for port-access

     authentication must be enabled on the switch.
     If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic

     VLAN for authentication sessions on the switch, the authentication fails.
  2. After you enable dynamic VLAN assignment in an authentication session, it is
     recommended that you use the interface unknown-vlans command on a per-port basis
  to
     prevent denial-of-service attacks. The interface unknown-vlans command allows you
   to:
  ```

```
    -Disable the port from sending advertisements of existing GVRP-created VLANs on
     the switch.
    -Drop all GVRP advertisements received on the port.

3. If you disable the use of dynamic VLANs in an authentication session using the
   no aaa port-access gvrp-vlans command, client sessions that were authenticated
   with a dynamic VLAN continue and are not deauthenticated. However, if a
   RADIUS-configured dynamic VLAN used for an authentication session is deleted
   from the switch through normal GVRP operation (for example, if no GVRP
  advertisements for the VLAN are received on any switch port), authenticated clients

   using this VLAN are deauthenticated.
```

held-period

- aaa port-access supplicant *[ETHERNET] PORT-LIST* held-period *< 0 to 65535 >*

  ```
  Set the held period (default 60sec.).
  ```

  Range: < 0 to 65535 >

identity

- aaa port-access supplicant *[ETHERNET] PORT-LIST* identity *IDENTITY*

  ```
  Set the identity(user name) to be used by the supplicant.
  ```

  Next Available Option:
  - **secret** -- **(p. 49)**

initialize

- aaa port-access authenticator *[ETHERNET] PORT-LIST* initialize

  ```
  Reinitialize the authenticator state machine.
  ```

- aaa port-access supplicant *[ETHERNET] PORT-LIST* initialize

  ```
  Reinitialize the supplicant state machine.
  ```

login

- aaa authentication console login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication telnet login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication web login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication ssh login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | tacacs | radius | ... > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa authentication login

  ```
  Usage: [no] aaa authentication login privilege-mode

  Description: Specify that switch respects the
               authentication server's privilege level.
  ```

  Next Available Option:
  - **privilege-mode** -- Specify that switch respects the authentication server's privilege level**(p. 46)**

logoff-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* logoff-period *< 1 to 999999999 >*

  ```
  Set period of time after which a client will be considered removed from the
  port for a lack of activity.
  ```

  Range: < 1 to 999999999 >
- aaa port-access mac-based *[ETHERNET] PORT-LIST* logoff-period *< 1 to 9999999 >*

  ```
  Set the period of time of inactivity that the switch considers an implicit logoff
  (default 300 seconds).
  ```

  Range: < 1 to 9999999 >
- aaa port-access web-based *[ETHERNET] PORT-LIST* logoff-period *< 1 to 9999999 >*

  ```
  Set the period of time of inactivity that the switch considers an implicit logoff
  (default 300 seconds).
  ```

  Range: < 1 to 9999999 >

mac-based

- aaa authentication mac-based

  ```
  Usage: aaa authentication mac-based <primary-method> [<backup-method>]

  Description: Configure authentication mechanism used to control mac-based
               port access to the switch.
  Parameters:
  ```

```
          o <primary-method> - Specifies the primary authentication
                               method for access control. Use <TAB>
                               or <?> after you specify enable or login
                               to get a list of all available
                               primary authentication methods.
          o <backup-method> -  Specifies an authentication method
                               to use, if the primary authentication
                               method is not able to check user's
                               credentials.
                               Use <TAB> or <?> after you specify the
                               primary authentication method to get a list
                               of all available backup methods.
```

Next Available Option:

- **primary** < chap-radius | peap-mschapv2 > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa port-access mac-based

```
Usage:  [no] aaa port-access mac-based
         addr-format <no-delimiter | single-dash | multi-dash |
              multi-colon | no-delimiter-uppercase | single-dash-uppercase |
              multi-dash-uppercase | multi-colon-uppercase>

        [no] aaa port-access mac-based [ethernet] PORT-LIST
        [addr-limit <1-32> | addr-moves | quiet-period <1-65535> |
         server-timeout <1-300> | max-requests <1-10> |
         logoff-period <1-9999999> | reauth-period <0-9999999>
         auth-vid VLAN-ID | unauth-vid VLAN-ID |
         reauthenticate]

Description: Configure MAC address based network authentication
             on the device or the device's port(s).

             The first form of the command sets the
             MAC address format which is common to all ports

             The second form of the command enables, disables, or
             configures authentication on the device's individual ports.

             o 'addr-format' sets the MAC address format to be used in the
               RADIUS request message (default no-delimiter).

             o 'addr-limit' sets the maximum number of MAC addresses to
               allow on the port. This includes ALL addresses (authenticated
               and unauthenticated). The default is 1 MAC address.
               NOTE: No more than 32 unique client MAC addresses can be
                     authorized by both 802.1X and MAC/web-based
                     authentication together on the same port.

             o 'addr-moves' sets whether the MAC address can move
               between ports that also have 'addr-moves' enabled
               (default disabled - no moves allowed).

             o 'quiet-period' sets the period of time during which the
               switch does not try to authenticate after a failed
               authentication attempt (default 60 seconds).
```

```
o 'server-timeout' sets the period of time after which the
  switch assumes that authentication has timed out
  (default 30 seconds).

o 'max-requests' sets the number of authentication attempts
  that must time out before authentication fails (default 3).

o 'logoff-period' sets the period of time of inactivity that
  the switch considers an implicit logoff (default 300).

o 'reauth-period' sets the period of time after which connected
  MAC addresses must be re-authenticated.  When set to 0
  the re-authentication is disabled (default 0).

o 'auth-vid' configures the VLAN to which to move a port
  after successful authentication.  RADIUS server can
  override the value.  Use 'no' form of the command to set
  this PVID to 0.  If the PVID is set to 0 no PVID changes
  occur unless RADIUS server requests.  Changes take effect
  immediately.  All clients must immediately re-authenticate.
  The default is 0.

o 'unauth-vid' configures the VLAN to which to move a port
  after failed authentication.  Use 'no' form of the command
  to set this PVID to 0.  Changes take effect immediately.
  The default is 0.

o 'reauthenticate' forces re-authentication
  of all clients present on a port.
```

Next Available Options:

- **mac-list1** -- Manage MAC address based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 38)**
- **addr-format** < no-delimiter | single-dash | multi-dash | ... > -- Set the MAC address format to be used in the RADIUS request message (default no-delimiter).**(p. 27)**

mac-list1

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST*

```
Manage MAC address based network authentication on the device port(s).
```

Next Available Options:

- **addr-limit** < 1 to 32 > -- Set the port's maximum number of authenticated MAC addresses (default 1). (NUMBER) **(p. 27)**
- **addr-moves** -- Set whether the MAC can move between ports (default disabled - no moves).**(p. 27)**
- **logoff-period** < 1 to 9999999 > -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 36)**
- **quiet-period** < 1 to 65535 > -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 46)**
- **server-timeout** < 1 to 300 > -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 49)**
- **max-requests** < 1 to 10 > -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 39)**

- **reauth-period** < 0 to 9999999 > -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 47)**
- **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default).**(p. 30)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default).**(p. 52)**
- **reauthenticate** -- Force re-authentication to happen.**(p. 47)**

max-requests

- aaa port-access authenticator *[ETHERNET] PORT-LIST* max-requests *< 1 to 10 >*

  ```
  Set maximum number of times the switch retransmits
  authentication requests (default 2).
  ```

  Range: < 1 to 10 >
- aaa port-access mac-based *[ETHERNET] PORT-LIST* max-requests *< 1 to 10 >*

  ```
  Set maximum number of times the switch retransmits authentication requests (default
  3).
  ```

  Range: < 1 to 10 >
- aaa port-access web-based *[ETHERNET] PORT-LIST* max-requests *< 1 to 10 >*

  ```
  Set maximum number of times the switch retransmits authentication requests (default
  3).
  ```

  Range: < 1 to 10 >

max-retries

- aaa port-access web-based *[ETHERNET] PORT-LIST* max-retries *< 1 to 10 >*

  ```
  Set number of times a client can enter their credentials before authentication is
  considered to have failed (default 3).
  ```

  Range: < 1 to 10 >

max-start

- aaa port-access supplicant *[ETHERNET] PORT-LIST* max-start *< 1 to 10 >*

  ```
  Define the maximum number of attempts taken to start authentication
  (default 3).
  ```

  Range: < 1 to 10 >

method

- aaa accounting commands *< stop-only >* *< radius >*

  ```
  Specify which accounting method to use (radius)
  ```

  Supported Values:
  - **radius** -- Use RADIUS protocol as accounting method.
- aaa accounting exec *< start-stop | stop-only >* *< radius >*

  ```
  Specify which accounting method to use (radius)
  ```

  Supported Values:

  - **radius** -- Use RADIUS protocol as accounting method.
- aaa accounting network *< start-stop | stop-only >* *< radius >*

  ```
  Specify which accounting method to use (radius)
  ```

  Supported Values:
  - **radius** -- Use RADIUS protocol as accounting method.
- aaa accounting system *< start-stop | stop-only >* *< radius >*

  ```
  Specify which accounting method to use (radius)
  ```

  Supported Values:
  - **radius** -- Use RADIUS protocol as accounting method.

mode

- aaa accounting commands *< stop-only >*

  ```
  Specify how to initiate and terminate an accounting session.
  ```

  Supported Values:
  - **stop-only** -- Send stop record accounting notice.

  Next Available Option:
  - **method** < radius > -- Specify which accounting method to use (radius) **(p. 39)**

- aaa accounting exec *< start-stop | stop-only >*

  ```
  Specify how to initiate and terminate an accounting session.
  ```

  Supported Values:
  - **start-stop** -- Send start and stop record accounting notice.
  - **stop-only** -- Send stop record accounting notice only.

  Next Available Option:
  - **method** < radius > -- Specify which accounting method to use (radius) **(p. 39)**

- aaa accounting network *< start-stop | stop-only >*

  ```
  Specify how to initiate and terminate an accounting session.
  ```

  Supported Values:
  - **start-stop** -- Send start and stop record accounting notice.
  - **stop-only** -- Send stop record accounting notice only.

  Next Available Option:
  - **method** < radius > -- Specify which accounting method to use (radius) **(p. 39)**

- aaa accounting system *< start-stop | stop-only >*

  ```
  Specify how to initiate and terminate an accounting session.
  ```

  Supported Values:
  - **start-stop** -- Send start and stop record accounting notice.
  - **stop-only** -- Send stop record accounting notice only.

Next Available Option:

- **method** < radius > -- Specify which accounting method to use (radius) **(p. 39)**

network

- [no] aaa accounting network

```
Usage: [no] aaa accounting network <start-stop|stop-only>
                                   <radius>

Description: Configure 'network' type of accounting.
Parameters:
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end
                           of the accounting session. Do not wait for
                           acknowledgement.
            o stop-only  - Send a stop record accounting notice at the end
                           of the accounting session.Do not wait for
                           acknowledgement.
            o radius     - Use RADIUS as the accounting protocol
```

Next Available Option:

- **mode** < start-stop | stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 40)**

null-username

- [no] aaa accounting suppress null-username

```
Do not generate accounting records for users with a null-username.
```

num-attempts

- aaa authentication num-attempts *< 1 to 10 >*

```
Usage: aaa authentication num-attempts <1-10>

Description: Specify the maximum number of login attempts
             allowed. The default value is 3.
```

Range: < 1 to 10 >

NUMBER-OF-CLIENTS

- aaa port-access authenticator *[ETHERNET] PORT-LIST* client-limit *< 1 to 32 >*

```
Set the maximum number of clients to allow on the port.
```

Range: < 1 to 32 >

periodic

- aaa accounting update periodic *< 1 to 525600 >*

```
Usage: [no] aaa accounting update periodic <number>

Description: Configure update accounting records mechanism.
Parameters:
```

```
              periodic <number> - Send accounting update records at regular
                                  intervals given by 'number' (in minutes).
```

Range: < 1 to 525600 >

port-access

- aaa authentication port-access

```
Usage: aaa authentication port-access ...

Description: Configure authentication mechanism used to control access
             to the network. The configured authentication method will.
             be used to authenticate 802.1X (Port Based Network Access
             Control Protocol) clients. The command should be followed
             by a keyword identifying an authentication method
             to use for Port Based Network Access Control Protocol clients
             authentication. Use 'aaa authentication port-access ?'
             to get a list of all available authentication methods.
```

Next Available Option:

- **primary** < local | eap-radius | chap-radius > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa port-access

```
Usage: [no] aaa port-access <authenticator ... | supplicant ...
                             web-based ... | mac-based ...>

Description: Configure 802.1X (Port Based Network Access),
             MAC address based network access,
             or web authentication based network access
             on the device.  You can configure authenticator,
             supplicant, MAC address based, or web authentication based
             network access on the device or device ports by specifying
             a corresponding keyword.
             See 'aaa port-access authenticator help', 'aaa port-access
             supplicant help', 'aaa port-access mac-based help', and
             'aaa port-access web-based help' for further details on
             authenticator, supplicant, MAC address based, and
             web authentication based network access configuration.
```

Next Available Options:

- **gvrp-vlans** -- Enable/disable the use of RADIUS-assigned dynamic (GVRP) VLANs**(p. 34)**
- **authenticator** -- Configure 802.1X authentication. **(p. 28)**
- **supplicant** -- Manage 802.1X supplicant. ([ethernet] PORT-LIST) **(p. 50)**
- **mac-based** -- Configure MAC address based network authentication on the device or the device's port(s)**(p. 36)**
- **web-based** -- Configure web authentication based network authentication on the device or the device's port(s)**(p. 54)**
- **PORT-LIST** -- Manage general port security features on the device port(s). ([ethernet] PORT-LIST) **(p. 42)**

PORT-LIST

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST*

```
Manage 802.1X on the device port(s).
```

Next Available Options:

- **control** < authorized | auto | unauthorized > -- Set the authenticator to Force Authorized, Force Unauthorized or Auto state (default Auto). (NUMBER) **(p. 32)**
- **quiet-period** < 0 to 65535 > -- Set the period of time the switch does not try to acquire a supplicant (default 60 sec.). (NUMBER) **(p. 46)**
- **tx-period** < 1 to 65535 > -- Set the period of time the switch waits until retransmission of EAPOL PDU (default 30 sec.). (NUMBER) **(p. 52)**
- **supplicant-timeout** < 1 to 300 > -- Set the supplicant response timeout on an EAP request (default 30 sec.). (NUMBER) **(p. 51)**
- **server-timeout** < 1 to 300 > -- Set the authentication server response timeout (default 30sec.). (NUMBER) **(p. 49)**
- **max-requests** < 1 to 10 > -- Set maximum number of times the switch retransmits authentication requests (default 2). (NUMBER) **(p. 39)**
- **reauth-period** < 0 to 9999999 > -- Set the re-authentication timeout (in seconds, default 0); set to '0' to disable re-authentication. (NUMBER) **(p. 47)**
- **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default).**(p. 30)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default).**(p. 52)**
- **unauth-period** < 0 to 255 > -- Set period of time the switch waits for authentication before moving the port to the VLAN for unauthenticated clients. (NUMBER) **(p. 52)**
- **logoff-period** < 1 to 999999999 > -- Set period of time after which a client will be considered removed from the port for a lack of activity. (NUMBER) **(p. 36)**
- **client-limit** -- Set the maximum number of clients to allow on the port.**(p. 31)**
- **initialize** -- Reinitialize the authenticator state machine.**(p. 35)**
- **reauthenticate** -- Force re-authentication to happen.**(p. 47)**
- **clear-statistics** -- Clear the authenticator statistics.**(p. 31)**

- [no] aaa port-access *[ETHERNET] PORT-LIST*

```
Manage general port security features on the device port(s).
```

Next Available Option:

- **controlled-direction** < both | in > -- Configure how traffic is controlled on non-authenticated ports; in BOTH directions (ingress+egress) or IN only (ingress). (NUMBER) **(p. 33)**

primary

- aaa authentication console enable < *local* | *tacacs* | *radius* >

```
Specify the primary authentication method for access control.
```

Supported Values:

- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.

Next Available Option:

- **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication console login *< local | tacacs | radius >*

  `Specify the primary authentication method for access control.`

  Supported Values:
  - **local** -- Use local switch user/password database.
  - **tacacs** -- Use TACACS+ server.
  - **radius** -- Use RADIUS server.

  Next Available Option:
  - **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication telnet enable *< local | tacacs | radius >*

  `Specify the primary authentication method for access control.`

  Supported Values:
  - **local** -- Use local switch user/password database.
  - **tacacs** -- Use TACACS+ server.
  - **radius** -- Use RADIUS server.

  Next Available Option:
  - **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication telnet login *< local | tacacs | radius >*

  `Specify the primary authentication method for access control.`

  Supported Values:
  - **local** -- Use local switch user/password database.
  - **tacacs** -- Use TACACS+ server.
  - **radius** -- Use RADIUS server.

  Next Available Option:
  - **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication web enable *< local | radius >*

  `Specify the primary authentication method for access control.`

  Supported Values:
  - **local** -- Use local switch user/password database.
  - **radius** -- Use RADIUS server.

  Next Available Option:
  - **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication web login *< local | radius >*

```
Specify the primary authentication method for access control.
```

Supported Values:

- **local** -- Use local switch user/password database.
- **radius** -- Use RADIUS server.

Next Available Option:

- **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication ssh enable < *local* | *tacacs* | *radius* | *...* >

```
Specify the primary authentication method for access control.
```

Supported Values:

- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.
- **public-key** -- Use local switch public key authentication database.

Next Available Option:

- **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication ssh login < *local* | *tacacs* | *radius* | *...* >

```
Specify the primary authentication method for access control.
```

Supported Values:

- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.
- **public-key** -- Use local switch public key authentication database.

Next Available Option:

- **secondary** < local | none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication port-access < *local* | *eap-radius* | *chap-radius* >

```
Specify the primary authentication method for access control.
```

Supported Values:

- **local** -- Use local switch user/password database.
- **eap-radius** -- Use EAP capable RADIUS server.
- **chap-radius** -- Use CHAP (MD5) capable RADIUS server.

Next Available Option:

- **secondary** < none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication web-based < *chap-radius* | *peap-mschapv2* >

```
Specify the primary authentication method for access control.
```

Supported Values:

- **chap-radius** -- Use RADIUS server with CHAP.
- **peap-mschapv2** -- Use RADIUS server with PEAP-MSChapv2.

Next Available Option:

- **secondary** < none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

- aaa authentication mac-based *< chap-radius | peap-mschapv2 >*

  ```
  Specify the primary authentication method for access control.
  ```

  Supported Values:

  - **chap-radius** -- Use RADIUS server with CHAP.
  - **peap-mschapv2** -- Use RADIUS server with PEAP-MSChapv2.

  Next Available Option:

  - **secondary** < none | authorized > -- Specify the backup authentication method for access control.**(p. 47)**

primary_method

- aaa authorization commands *< radius | none >*

  Supported Values:

  - **radius** -- Use RADIUS protocol as the authorization method.
  - **none** -- No authorization (always succeeds).

privilege-mode

- [no] aaa authentication login privilege-mode

  ```
  Usage: [no] aaa authentication login privilege-mode

  Description: Specify that switch respects the
               authentication server's privilege level.
  ```

quiet-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* quiet-period *< 0 to 65535 >*

  ```
  Set the period of time the switch does not try to
  acquire a supplicant (default 60 sec.).
  ```

  Range: < 0 to 65535 >

- aaa port-access mac-based *[ETHERNET] PORT-LIST* quiet-period *< 1 to 65535 >*

  ```
  Set the period of time the switch does not try to authenticate (default 60 seconds).
  ```

  Range: < 1 to 65535 >

- aaa port-access web-based *[ETHERNET] PORT-LIST* quiet-period *< 1 to 65535 >*

  ```
  Set the period of time the switch does not try to authenticate (default 60 seconds).
  ```

  Range: < 1 to 65535 >

reauthenticate

- aaa port-access authenticator *[ETHERNET] PORT-LIST* reauthenticate

  ```
  Force re-authentication to happen.
  ```

- aaa port-access mac-based *[ETHERNET] PORT-LIST* reauthenticate

  ```
  Force re-authentication to happen.
  ```

- aaa port-access web-based *[ETHERNET] PORT-LIST* reauthenticate

  ```
  Force re-authentication to happen.
  ```

reauth-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* reauth-period *< 0 to 9999999 >*

  ```
  Set the re-authentication timeout (in seconds,
  default 0); set to '0' to disable re-authentication.
  ```

  Range: < 0 to 9999999 >
- aaa port-access mac-based *[ETHERNET] PORT-LIST* reauth-period *< 0 to 9999999 >*

  ```
  Set the re-authentication timeout in seconds; set to '0' to disable re-authentication
   (default 0).
  ```

  Range: < 0 to 9999999 >
- aaa port-access web-based *[ETHERNET] PORT-LIST* reauth-period *< 0 to 9999999 >*

  ```
  Set the re-authentication timeout in seconds; set to '0' to disable re-authentication
   (default 0).
  ```

  Range: < 0 to 9999999 >

redirect-url

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* redirect-url

  ```
  Set the URL that the user should be redirected to after successful login (default
  none), Specify url up to 103 characters length.
  ```

  Next Available Option:
  - **web-redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length. (ASCII-STR) **(p. 57)**

secondary

- aaa authentication console enable *< local | tacacs | radius >* *< local | none | authorized >*

  ```
  Specify the backup authentication method for access control.
  ```

  Supported Values:
  - **local** -- Use local switch user/password database.
  - **none** -- Do not use backup authentication methods.
  - **authorized** -- Allow access without authentication.
- aaa authentication console login *< local | tacacs | radius >* *< local | none | authorized >*

  ```
  Specify the backup authentication method for access control.
  ```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication telnet enable *< local | tacacs | radius >* *< local | none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication telnet login *< local | tacacs | radius >* *< local | none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication web enable *< local | radius >* *< local | none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication web login *< local | radius >* *< local | none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication ssh enable *< local | tacacs | radius | ... >* *< local | none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication ssh login *< local | tacacs | radius | ... >* *< local | none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.
- **authorized** -- Allow access without authentication.

- aaa authentication port-access *< local | eap-radius | chap-radius >* *< none | authorized >*

```
Specify the backup authentication method for access control.
```

Supported Values:

  - **none** -- Do not use backup authentication methods.
  - **authorized** -- Allow access without authentication.
- aaa authentication web-based *< chap-radius | peap-mschapv2 >* *< none | authorized >*

  ```
  Specify the backup authentication method for access control.
  ```

  Supported Values:
  - **none** -- Do not use backup authentication methods.
  - **authorized** -- Allow access without authentication.
- aaa authentication mac-based *< chap-radius | peap-mschapv2 >* *< none | authorized >*

  ```
  Specify the backup authentication method for access control.
  ```

  Supported Values:
  - **none** -- Do not use backup authentication methods.
  - **authorized** -- Allow access without authentication.

secret

- aaa port-access supplicant *[ETHERNET] PORT-LIST* identity *IDENTITY* secret
- aaa port-access supplicant *[ETHERNET] PORT-LIST* secret

  ```
  Trigger the command to ask user for a password for the supplicant to use.
  ```

server-timeout

- aaa port-access authenticator *[ETHERNET] PORT-LIST* server-timeout *< 1 to 300 >*

  ```
  Set the authentication server response timeout (default 30sec.).
  ```

  Range: < 1 to 300 >
- aaa port-access mac-based *[ETHERNET] PORT-LIST* server-timeout *< 1 to 300 >*

  ```
  Set the authentication server response timeout (default 30 seconds).
  ```

  Range: < 1 to 300 >
- aaa port-access web-based *[ETHERNET] PORT-LIST* server-timeout *< 1 to 300 >*

  ```
  Set the authentication server response timeout (default 30 seconds).
  ```

  Range: < 1 to 300 >

ssh

- aaa authentication ssh

  ```
  Usage: aaa authentication ssh <enable|login>
                                  <primary-method> [<backup-method>]

  Description: Configure authentication mechanism used to control SSH
               access to the switch.
  Parameters:
              o enable           - Configure access to privileged mode.
              o login            - Configure login access.
              o <primary-method> - Specifies the primary authentication
                                   method for access control. Use <TAB>
                                   or <?> after you specify enable or login
                                   to get a list of all available
                                   primary authentication methods.
              o <backup-method> -  Specifies an authentication method
  ```

```
                                    to use, if the primary authentication
                                    method is not able to check user's
                                    credentials.
                                    Use <TAB> or <?> after you specify the
                                    primary authentication method to get a list
                                    of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 33)**
- **login** -- Configure login access to the switch.**(p. 35)**

ssl-login

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* ssl-login

```
Set whether to enable SSL login (https on port 443) (default disabled).
```

start-period

- aaa port-access supplicant *[ETHERNET] PORT-LIST* start-period *< 1 to 300 >*

```
Set a period of time between EAPOL-Start packet retransmission
(default 30sec.).
```

Range: < 1 to 300 >

supplicant

- [no] aaa port-access supplicant *[ETHERNET] PORT-LIST*

```
Usage: [no] aaa port-access supplicant [ethernet] PORT-LIST
       [auth-timeout <1-300> | held-period <0-65535> |
        start-period <1-300> | max-start <1-10> |
        identity <identity> [secret] | secret
        initialize | reauthenticate | clear-statistics]

Description: Manage 802.1X (Port Based Network Access) supplicant
             on the device ports. Called without the optional parameters
             the command enables or disables (if 'no' is specified) the
             supplicant functionality on the specified ports.
             The 'no' keyword can not be used with any of the
             optional parameters. All changes made by the command apply
             to the specified PORT-LIST only.
             o 'auth-timeout' sets the period of time the supplicant waits
               to receive a challenge from the authenticator
               (default 30sec.).
             o 'held-period' sets a period of time the supplicant waits
               after receiving a failure before trying to re-acquire the
               authenticatior (default 60sec.).
             o 'start-period' sets a period of time between transmitting
               EAPOL-Start packets in Connecting state (default 30sec.).
             o 'max-start' defines the maximum number of attempts to
               start authentication before the supplicant assumes that
               it has been authenticated (default 3).
             o 'identity' sets the identity to be used by the port
               supplicant when MD5 authentication request is received
               from an authenticator.
             o 'secret' sets the secret to be used by the port
               supplicant when MD5 authentication request is received
```

```
                  from an authenticator. User will be prompted to enter
                  the secret after the command is invoked.
                o 'initialize' reinitializes supplicant's state machine.
                o 'clear-statistics' clears supplicant statistics counters.
```

Next Available Options:

- **auth-timeout** < 1 to 300 > -- Set the challenge reception timeout (default 30sec.). (NUMBER) **(p. 30)**
- **held-period** < 0 to 65535 > -- Set the held period (default 60sec.). (NUMBER) **(p. 35)**
- **start-period** < 1 to 300 > -- Set a period of time between EAPOL-Start packet retransmission (default 30sec.). (NUMBER) **(p. 50)**
- **max-start** < 1 to 10 > -- Define the maximum number of attempts taken to start authentication (default 3). (NUMBER) **(p. 39)**
- **initialize** -- Reinitialize the supplicant state machine.**(p. 35)**
- **identity** -- Set the identity(user name) to be used by the supplicant. (ASCII-STR) **(p. 35)**
- **secret** -- Trigger the command to ask user for a password for the supplicant to use.**(p. 49)**
- **clear-statistics** -- Clear the supplicant statistics.**(p. 31)**

supplicant-timeout

- aaa port-access authenticator *[ETHERNET] PORT-LIST* supplicant-timeout *< 1 to 300 >*

```
Set the supplicant response timeout on an EAP request
(default 30 sec.).
```

Range: < 1 to 300 >

suppress

- [no] aaa accounting suppress

```
Do not generate accounting records for a specific type of user.
```

Next Available Option:

- **null-username** -- Do not generate accounting records for users with a null-username. **(p. 41)**

system

- [no] aaa accounting system

```
Usage: [no] aaa accounting system  <start-stop|stop-only>
                                   <radius>

Description: Configure 'system' type of accounting.
Parameters:
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end
                           of the accounting session. Do not wait for
                           acknowledgement.
            o stop-only  - Send a stop record accounting notice at the end
                           of the accounting session.Do not wait for
                           acknowledgement.
            o radius     - Use RADIUS as the accounting protocol
```

Next Available Option:

- **mode** < start-stop | stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 40)**

telnet

- aaa authentication telnet

```
Usage: aaa authentication telnet <enable|login>
                                 <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control telnet
             access to the switch.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
                                 primary authentication method to get a list
                                 of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 33)**
- **login** -- Configure login access to the switch.**(p. 35)**

tx-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* tx-period *< 1 to 65535 >*

```
Set the period of time the switch waits until
retransmission of EAPOL PDU (default 30 sec.).
```

Range: < 1 to 65535 >

unauth-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* unauth-period *< 0 to 255 >*

```
Set period of time the switch waits for authentication before moving the
port to the VLAN for unauthenticated clients.
```

Range: < 0 to 255 >

unauth-vid

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST* unauth-vid

```
Configures VLAN where to keep port while there is an unauthenticated client connected
 (not configured by default).
```

Next Available Option:

- **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default). (VLAN-ID) **(p. 53)**

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST* unauth-vid

  ```
  Configures VLAN where to keep port while there is an unauthorized client connected
  (not configured by default).
  ```

  Next Available Option:

  - **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 53)**

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* unauth-vid

  ```
  Configures VLAN where to keep port while there is an unauthorized client connected
  (not configured by default).
  ```

  Next Available Option:

  - **web-unauthvid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 57)**

update

- [no] aaa accounting update

  ```
  Usage: [no] aaa accounting update periodic <number>

  Description: Configure update accounting records mechanism.
  Parameters:
                periodic <number> - Send accounting update records at regular
                                    intervals given by 'number' (in minutes).
  ```

  Next Available Option:

  - **periodic** < 1 to 525600 > -- Configure update accounting records mechanism**(p. 41)**

VLAN-ID

- aaa port-access authenticator *[ETHERNET] PORT-LIST* auth-vid *VLAN-ID*

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

- aaa port-access authenticator *[ETHERNET] PORT-LIST* unauth-vid *VLAN-ID*

  ```
  Configures VLAN where to keep port while there is an unauthenticated client connected
   (not configured by default).
  ```

- aaa port-access mac-based *[ETHERNET] PORT-LIST* auth-vid *VLAN-ID*

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

- aaa port-access mac-based *[ETHERNET] PORT-LIST* unauth-vid *VLAN-ID*

```
Configures VLAN where to keep port while there is an unauthorized client connected
(not configured by default).
```

web

- aaa authentication web

```
Usage: aaa authentication web <enable|login>
                                 <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control web
             access to the switch.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
                                 primary authentication method to get a list
                                 of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 33)**
- **login** -- Configure login access to the switch.**(p. 35)**

web-authvid

- aaa port-access web-based *[ETHERNET] PORT-LIST* auth-vid *VLAN-ID*

```
Configures VLAN where to move port after successful authentication (not configured
by default).
```

web-based

- aaa authentication web-based

```
Usage: aaa authentication web-based <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control web-based
             port access to the switch.
Parameters:
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
```

```
                                primary authentication method to get a list
                                of all available backup methods.
```

Next Available Option:

- **primary** < chap-radius | peap-mschapv2 > -- Specify the primary authentication method for access control.**(p. 43)**

- aaa port-access web-based

```
Usage:   [no] aaa port-access web-based
         [dhcp-addr <base address / mask> | dhcp-lease <5-25>]

         [no] aaa port-access web-based [ethernet] PORT-LIST
         [client-limit <1-32> | client-moves | ssl-login |
          redirect-url <URL> | quiet-period <1-65535> |
          server-timeout <1-300> | max-requests <1-10> |
          max-retries <1-10> | logoff-period <1-9999999> |
          reauth-period <0-9999999> | auth-vid VLAN-ID |
          unauth-vid VLAN-ID | reauthenticate]

Description: Configure web authentication based network authentication
             on the device or the device's port(s).

             The first form of the command sets the dhcp address
             or lease parameter which are common to all ports

             The second form of the command enables, disables, or
             configures authentication on the device's individual ports.

             o 'dhcp-addr' sets the base address / mask for the temporary
               pool used by DHCP (base address default is 192.168.0.0,
               mask default is 24 - 255.255.255.0)

             o 'dhcp-lease' sets the lease length of the temporary
               IP address issued by DHCP (default 10)

             o 'client-limit' sets the maximum number of clients to allow on
               the port. This includes ALL clients (authenticated and
               unauthenticated). The default is 1 client.
               NOTE: No more than 32 unique client MAC addresses can be
                     authorized by both 802.1X and MAC/web-based
                     authentication together on the same port.

             o 'client-moves' sets whether the client can move
               between ports that also have 'client-moves' enabled
               (default disabled - no moves allowed).

             o 'ssl-login' sets whether to enable SSL logins (https on
               port 443).  If enabled, logins to plaintext http (port 80)
               are redirected to https port.  The default is disabled.

             o 'redirect-url' sets the URL that the user should be
               redirected to after successful login (default none)
               Specify url up to 103 characters length.

             o 'quiet-period' sets the period of time during which the
               switch does not try to authenticate after a failed
               authentication attempt (default 60 seconds).
```

```
o 'server-timeout' sets the period of time after which the
  switch assumes that authentication has timed out
  (default 30 seconds).

o 'max-requests' sets the number of authentication attempts
  that must time out before authentication fails (default 3)

o 'max-retries' sets number of times a client can enter
  their credentials before authentication is considered
  to have failed (default 3).

o 'logoff-period' sets the period of time of inactivity that
  the switch considers an implicit logoff (default 300)

o 'reauth-period' sets the period of time after which connected
  clients must be re-authenticated.  When the timeout is set
  to 0 the re-authentication is disabled (default 0).

o 'auth-vid' configures the VLAN to which to move a port
  after successful authentication.  RADIUS server can
  override the value.  Use 'no' form of the command to set
  this PVID to 0.  If the PVID is set to 0 no PVID changes
  occur unless RADIUS server requests.  Changes take effect
  immediately.  All clients must immediately re-authenticate.
  The default is 0.

o 'unauth-vid' configures the VLAN to which to move a port
  after failed authentication.  Use 'no' form of the command
  to set this PVID to 0.  Changes take effect immediately.
  The default is 0.

o 'reauthenticate' forces re-authentication
  of all clients present on a port.
```

Next Available Options:

- **web-list1** -- Manage web authentication based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 56)**
- **dhcp-addr** -- Set the base address / mask for the temporary pool used by DHCP (base address default is 192.168.0.0, mask default is 24 - 255.255.255.0). (IP-ADDR/MASK-LENGTH) **(p. 33)**
- **dhcp-lease** < 5 to 25 > -- Set the lease length of the IP address issued by DHCP (default 10). (NUMBER) **(p. 33)**

web-list1

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST*

```
Manage web authentication based network authentication on the device port(s).
```

Next Available Options:

- **client-limit** < 1 to 32 > -- Set the port's maximum number of authenticated clients (default 1). (NUMBER) **(p. 31)**
- **client-moves** -- Set whether the client can move between ports (default disabled - no moves).**(p. 31)**
- **ssl-login** -- Set whether to enable SSL login (https on port 443) (default disabled).**(p. 50)**

- **redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length.**(p. 47)**
- **max-retries** < 1 to 10 > -- Set number of times a client can enter their credentials before authentication is considered to have failed (default 3). (NUMBER) **(p. 39)**
- **logoff-period** < 1 to 9999999 > -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 36)**
- **quiet-period** < 1 to 65535 > -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 46)**
- **server-timeout** < 1 to 300 > -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 49)**
- **max-requests** < 1 to 10 > -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 39)**
- **reauth-period** < 0 to 9999999 > -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 47)**
- **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default).**(p. 30)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default).**(p. 52)**
- **reauthenticate** -- Force re-authentication to happen.**(p. 47)**

web-redirect-url

- aaa port-access web-based *[ETHERNET] PORT-LIST* redirect-url *WEB-REDIRECT-URL*

```
Set the URL that the user should be redirected to after successful login (default
none), Specify url up to 103 characters length.
```

web-unauthvid

- aaa port-access web-based *[ETHERNET] PORT-LIST* unauth-vid *VLAN-ID*

```
Configures VLAN where to keep port while there is an unauthorized client connected
(not configured by default).
```

arp

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: no arp IP-ADDRESS

Description: Remove the specified IP-ADDRESS entry from the ARP cache
             (note: the keyword 'no' must be specified).

     o   IP-ADDRESS - ip address of the ARP cache entry to be removed.
```

COMMAND STRUCTURE

arp-protect

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] arp-protect [trust [ethernet] PORT-LIST|
                        validate <ip|destination-mac|src-mac>|
                        vlan VLAN-ID-RANGE]

Description: Configure Dynamic ARP Protection.
             To Enable/disable ARP Protection on the switch execute the
             [no] arp-protect command. Dynamic ARP Protection will not be
             enabled on any VLAN if it is not enabled on the switch.
             By default Dynamic ARP Protection is disabled.
             To configure which VLANs are to be protected execute the
             'arp-protect vlan' command. By default Dynamic ARP Protection
             is disabled on all VLANs.

             Dynamic ARP Protection divides ports into two categories:
             untrusted and trusted. ARP packets received on trusted ports
             are forwarded without validation.
             ARP packets received on the untrusted ports of a protected VLAN
             are intercepted and validated before being forwarded.
             By default ports are untrusted.

             Dynamic ARP Protection validates ARP packets based on the
             IP-to-MAC binding database maintained by DHCP snooping. If DHCP
             snooping is not enabled then a loss of connectivity will result
             since the database will contain no bindings. For devices that do
             not use DHCP to obtain their IP configuration static bindings can
             be added manually to the database with the 'ip source-binding'
             command.

             Dynamic ARP Protection can also be configured to drop ARP packets
             that contain invalid IP addresses or when the MAC addresses in the
             body of the ARP packet do not match those in the ethernet header.

Parameters:
      trust [ethernet] PORT-LIST     -- Configure ports as trusted or untrusted.
      validate <ip|dest-mac|src-mac> -- Configure addiional ARP packet checks.
      vlan VLAN-ID-RANGE             -- Enable/disable ARP Protection on VLANs
```

COMMAND STRUCTURE

- [no] arp-protect **trust** -- Configure port(s) as trusted or untrusted. ([ethernet] PORT-LIST) **(p. 60)**
- [no] arp-protect **validate** -- Configure additional ARP Protection validation checks. **(p. 60)**
  - **dest-mac** -- Drop any ARP response packet in which the destination MAC address in the ethernet header does not match the target MAC address in the body of the packet. **(p. 60)**
  - **ip** -- Drop any ARP request with an invalid sender IP address. Drop any ARP response with an invalid target IP address. Invalid IP addresses include 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all class E IP addresses. **(p. 60)**

  - **src-mac** -- Drop any ARP request or response packet in which the source MAC in the ethernet header does not match the sender MAC address in the body of the packet. **(p. 60)**
- [no] arp-protect **vlan** -- Enable/disable Dynamic ARP Protection on a VLAN(s). **(p. 61)**
  - **vlan-list** -- (VLAN-ID-RANGE) **(p. 61)**

COMMAND DETAILS

dest-mac (p. 60)
ip (p. 60)
src-mac (p. 60)
trust (p. 60)
validate (p. 60)
vlan (p. 61)
vlan-list (p. 61)

dest-mac

- [no] arp-protect validate dest-mac

  Drop any ARP response packet in which the destination MAC address in the ethernet header does not match the target MAC address in the body of the packet.

ip

- [no] arp-protect validate ip

  Drop any ARP request with an invalid sender IP address. Drop any ARP response with an invalid target IP address. Invalid IP addresses include 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all class E IP addresses.

src-mac

- [no] arp-protect validate src-mac

  Drop any ARP request or response packet in which the source MAC in the ethernet header does not match the sender MAC address in the body of the packet.

trust

- [no] arp-protect trust *[ETHERNET] PORT-LIST*

  Configure port(s) as trusted or untrusted.

validate

- [no] arp-protect validate

  Configure additional ARP Protection validation checks.

  Next Available Options:

  - **src-mac** -- Drop any ARP request or response packet in which the source MAC in the ethernet header does not match the sender MAC address in the body of the packet. **(p. 60)**
  - **dest-mac** -- Drop any ARP response packet in which the destination MAC address in the ethernet header does not match the target MAC address in the body of the packet. **(p. 60)**
  - **ip** -- Drop any ARP request with an invalid sender IP address. Drop any ARP response with an invalid target IP address. Invalid IP addresses include 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all class E IP addresses. **(p. 60)**

vlan

- [no] arp-protect vlan

  ```
  Enable/disable Dynamic ARP Protection on a VLAN(s).
  ```

  Next Available Option:

  - **vlan-list** -- (VLAN-ID-RANGE) **(p. 61)**

vlan-list

- [no] arp-protect vlan *VLAN-ID-RANGE*

autorun

OVERVIEW

Category:	
Primary context:	config
Related Commands	**copy usb (page 131)**

```
Usage:  [no] autorun ...

Description: Enable/Disable/Configure Autorun. Use the 'secure-mode' keyword
             to enable/disable secure mode for autorun. Use the
             'encryption-key' keyword to configure or remove an encryption key
             (a base-64 encoded string). The encryption key is a prerequisite
             for enabling autorun in secure-mode. Encryption is noted only when
             the AutoRun file is also signed by an authentic source.
```

NOTES

Operating Notes

- Autorun is enabled by default, until passords are set on the device.
- Secure-mode and encryption-key are disabled by default.
- If secure mode is disabled, the key-pair can be removed using the crypto-key zeroize autorun command.
- When installing the autorun certificate file and/or other key files, the files must be in PEM format.

COMMAND STRUCTURE

- [no] autorun **encryption-key** -- Configure or remove an AES 128 encryption-key for Autorun **(p. 62)**
  - **key** -- AES 128 encryption key string for Autorun (ASCII-STR) **(p. 62)**
- [no] autorun **secure-mode** -- Enable or disable secure mode for Autorun. **(p. 63)**

COMMAND DETAILS

encryption-key (p. 62)	**key (p. 62)**	**secure-mode (p. 63)**

encryption-key

- [no] autorun encryption-key

```
Configure or remove an AES 128 encryption-key for Autorun
```

Next Available Option:

- **key** -- AES 128 encryption key string for Autorun (ASCII-STR) **(p. 62)**

key

- autorun encryption-key *KEY*

```
AES 128 encryption key string for Autorun
```

secure-mode

- [no] autorun secure-mode

```
Enable or disable secure mode for Autorun. Secure-mode can be enabled if an
encryption-key has already been configured and a trusted certificate for
verifying autorun command files has been copied to the switch using the
"copy <tftp | usb> autorun-cert-file" command.
```

auto-tftp

OVERVIEW

Category:	File Transfer
Primary context:	config
Related Commands	**the section called “client” (page 592)**

```
Usage: [no] auto-tftp [<IPV4-ADDR | IPV6-ADDR> <FILENAME-STR>]

Description: Enable/disable automatic software image download via TFTP during
             boot. The software image will be downloaded if it has a different
             version from the software running on the switch. The command requires
             the parameters to be specified when used without 'no'.
             o IPV4-ADDR - specifies the TFTP server IPv4 address to download
               a software image from.
             o IPV6-ADDR - specifies the TFTP server IPv6 address to download
               a software image from.
             o FILENAME-STR - specifies the file-name to download.
```

COMMAND STRUCTURE

- auto-tftp **server-ip** -- IPv4 address of the TFTP server to download a software image from. (IP-ADDR) **(p. 64)**
  - **filename** -- The software image file-name. (ASCII-STR) **(p. 64)**
- auto-tftp **server-ipv6** -- IPv6 address of the TFTP server to download a software image from. (IPV6-ADDR) **(p. 65)**
  - **filename** -- The software image file-name. (ASCII-STR) **(p. 64)**

EXAMPLES

Example: auto-tftp IP-ADDR FILENAME

Set the device to boot using image2 located on TFTP server 10.10.2.40, if the image version is different from the one already on the switch:

```
ProCurve(config)# auto-tftp 10.10.2.40 image2
```

COMMAND DETAILS

filename (p. 64)	**server-ip (p. 64)**	**server-ipv6 (p. 65)**

filename

- auto-tftp *IP-ADDR FILENAME*

```
The software image file-name.
```

- auto-tftp *IPV6-ADDR FILENAME*

```
The software image file-name.
```

server-ip

- auto-tftp *IP-ADDR*

```
IPv4 address of the TFTP server to download a software image from.
```

Next Available Option:

- **filename** -- The software image file-name. (ASCII-STR) **(p. 64)**

server-ipv6

- auto-tftp *IPV6-ADDR*

```
IPv6 address of the TFTP server to download a software image from.
```

Next Available Option:

- **filename** -- The software image file-name. (ASCII-STR) **(p. 64)**

banner

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show banner (page 457)**

```
Usage: [no] banner motd ASCII-STR

Description: Define a login banner. The banner will be displayed before
             login on the console, telnet, ssh, and Web-UI sessions.
             The banner can be a multi-line text up to 320 characters.
             The banner text can contain any printable character except
             the delimiting character and the ~ character.
```

COMMAND STRUCTURE

- [no] banner **motd** -- Set message of the day banner **(p. 66)**
  - **ascii** -- Specify delimiting character for banner text (ASCII-STR) **(p. 66)**

EXAMPLES

Example: banner motd DELIMITER

Configure a banner message that reads "Welcome to this ProCurve switch." and verify it:

```
ProCurve(config)# banner motd >
Enter TEXT message. End with the character'>'
Welcome to this ProCurve switch.>

ProCurve(config)# show banner motd
Banner Information Banner status: Enabled
Configured Banner:
Welcome to this ProCurve switch.
```

COMMAND DETAILS

ascii (p. 66)	**motd (p. 66)**

ascii

- banner motd *ASCII*

  ```
  Specify delimiting character for banner text
  ```

motd

- [no] banner motd

  ```
  Set message of the day banner
  ```

  Next Available Option:
  - **ascii** -- Specify delimiting character for banner text (ASCII-STR) **(p. 66)**

boot

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**reload (page 403)**

```
Usage: boot [system [flash <primary|secondary>] [config FILENAME]]
       boot set-default flash <primary|secondary>
       boot active
       boot standby

Description: Reboot the device. The primary or secondary software image
             can be specified to be used during the boot process.
             Optionally, a configuration file can be set for this boot.

Parameters:
    o set-default- Sets the default flash boot image for next boot.
    o active     - Causes switchover and reboots the  active management
                   module, if redundancy is enabled and the other module
                   is present. Reboots the system if redundancy is disabled
                   or the module is not present.
    o standby    - Reboots the standby management module.
```

COMMAND STRUCTURE

- boot **active** -- Reboot the active management module. **(p. 68)**
- boot **set-default** -- Specify the default flash boot image. **(p. 68)**
  - **flash < primary | secondary >** -- Specify the default flash boot image. **(p. 68)**
- boot **standby** -- Reboot the standby management module. **(p. 69)**
- boot **system** -- Allows user to specify boot image to use after reboot. **(p. 69)**
  - **flash < primary | secondary >** -- Specify boot image to use after reboot. **(p. 68)**
    - **config < config | new >** -- Specify configuration file to use on boot. **(p. 68)**

EXAMPLES

Example: boot

```
Boot the switch from primary flash with pending configuration changes
in the running-config file:

ProCurve(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
Boot from primary flash
Do you want to save current configuration [y/n]?
```

Example: boot system flash secondary

```
Reboot the switch from secondary flash when there are no pending configuration changes
in the running-config file:

ProCurve(config)# boot system flash secondary
Device will be rebooted, do you want to continue [y/n] ? y
Boot from secondary flash
Do you want to save current configuration [y/n]?
```

COMMAND DETAILS

active

- boot active

  Note: This command applies to the 8212zl switch only.

  Reboot the active management module. The switch starts to boot from the default flash image. You can select which image to boot from during the boot process itself. The switch will switchover to the standby management module. If a second management module is not present in the switch, the system is rebooted.

config

- boot system flash < *primary* | *secondary* > config < *config* | *new* >

  Specify configuration file to use on boot.

  Supported Values:
  - **config**
  - **new**

flash

- boot system flash < *primary* | *secondary* >

  Specify boot image to use after reboot.

  Supported Values:
  - **primary** -- Primary flash image.
  - **secondary** -- Secondary flash image.

  Next Available Option:
  - **config** < config | new > -- Specify configuration file to use on boot.**(p. 68)**

- boot set-default flash < *primary* | *secondary* >

  Specify the default flash boot image.

  Supported Values:
  - **primary** -- Primary flash image.
  - **secondary** -- Secondary flash image.

set-default

- boot set-default

  Specify the default flash boot image. Sets the default flash for the next boot to primary or secondary. You will see this message: "This command changes the location of the default boot. This command will change the default flash image to boot from <flash chosen>. Hereafter, 'reload' and 'boot' commands will boot from <flash chosen>. Do you want to continue [y/n]?"

Next Available Option:

- **flash** < primary | secondary > -- Specify the default flash boot image.**(p. 68)**

standby

- boot standby

```
Reboot the standby management module.  The switch does not switchover.
If the standby module is not present, this message displays: “The other
management module is not present.”
```

system

- boot system

```
Allows user to specify boot image to use after reboot.
```

Next Available Option:

- **flash** < primary | secondary > -- Specify boot image to use after reboot.**(p. 68)**

cdp

OVERVIEW

Category:	Routing
Primary context:	config
Related Commands	**show cdp (page 459)**

```
Usage: [no] cdp ...

Description: Set various CDP (Cisco Discovery Protocol) parameters. Use
             'cdp ?' to get a list of all possible options.
```

COMMAND STRUCTURE

- [no] cdp **enable** -- Enable/disable CDP on particular device ports ([ethernet] PORT-LIST) **(p. 70)**
- [no] cdp **run** -- Start and stop CDP on the device **(p. 70)**

EXAMPLES

Example: cdp enable PORT-LIST

Disable CDP on port A1 of a Series 5400zl switch:

```
ProCurve(config)# no cdp enable a1
```

Example: cdp run

Disable CDP on the switch:

```
ProCurve(config)# no cdp run
```

COMMAND DETAILS

enable (p. 70)	**run (p. 70)**

enable

- [no] cdp enable *[ETHERNET] PORT-LIST*

```
Usage: [no] cdp enable [ethernet] PORT-LIST

Description: Enable/disable CDP on particular device ports.
```

run

- [no] cdp run

```
Usage: [no] cdp run

Description: Start and stop CDP on the device.
```

chassislocate

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: chassislocate <on|blink> [<1-1440>]
       chassislocate off

Description: Control the chassis locate led.

Parameters:

    o on - Turn the led on.
    o off - Turn the led off.
    o blink - Make the led blink.
    o [<1-1440>] - Number of minutes the led is
                  to blink or be turned on (default is 30).
```

COMMAND STRUCTURE

- chassislocate **blink** -- Blink the chassis locate led (default 30 minutes). **(p. 71)**
  - **duration < 1 to 1440 >** -- Number of minutes duration (default 30). (NUMBER) **(p. 71)**
- chassislocate **off** -- Turn the chassis locate led off. **(p. 72)**
- chassislocate **on** -- Turn the chassis locate led on (default 30 minutes). **(p. 72)**
  - **duration < 1 to 1440 >** -- Number of minutes duration (default 30). (NUMBER) **(p. 71)**

COMMAND DETAILS

blink (p. 71)	**off (p. 72)**
duration (p. 71)	**on (p. 72)**

blink

- chassislocate blink

  ```
  Blink the chassis locate led (default 30 minutes).
  ```

  Next Available Option:

  - **duration** < 1 to 1440 > -- Number of minutes duration (default 30). (NUMBER) **(p. 71)**

duration

- chassislocate on *< 1 to 1440 >*

  ```
  Number of minutes duration (default 30).
  ```

  Range: < 1 to 1440 >
- chassislocate blink *< 1 to 1440 >*

  ```
  Number of minutes duration (default 30).
  ```

  Range: < 1 to 1440 >

off

- chassislocate off

```
Turn the chassis locate led off.
```

on

- chassislocate on

```
Turn the chassis locate led on (default 30 minutes).
```

Next Available Option:

- **duration** < 1 to 1440 > -- Number of minutes duration (default 30). (NUMBER) **(p. 71)**

clear

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: clear <arp|intrusion-log|logging|public-key|statistics
             [ethernet] PORT-LIST |link-keepalive statistics>

Description: Clear table/statistics or authorized client public keys.

Parameters:

    o arp - Flushes all non-permanent entries in the ARP cache.

    o intrusion-log - Resets the Alert Flags and prepares
      the switch to detect and log the next security intrusion.

    o logging - Remove all event entries from the event log

    o public-key - Removes currently loaded authorized client public keys
      from active configuration.

    o statistics PORT-LIST - Resets all port counters associated with
      the ports specified.

    o link-keepalive statistics - Resets the UDLD packets sent, UDLD
      packets received, and Transition counters for all UDLD enabled ports.
```

COMMAND STRUCTURE

- clear **arp** -- Flush all non-permanent entries in the ARP cache. **(p. 74)**
- clear **crypto** -- Remove client public keys from active configuration. **(p. 74)**
  - **client-public-key** -- Remove client public keys from active configuration. **(p. 74)**
    - **keyfile < manager | operator >** -- Remove client public keys from active configuration. **(p. 74)**
      - **keylist** -- Remove client public keys from active configuration. (ASCII-STR) **(p. 74)**
- clear **intrusion-flags** -- Reset the Alert Flag on all ports. **(p. 74)**
- clear **ipv6** -- Clear all IPv6 information. **(p. 74)**
  - **neighbors** -- Delete all the neighbour discovery cache entries, except static entries. **(p. 75)**
- clear **link-keepalive** -- Reset link-keepalive counters for all UDLD enabled ports. **(p. 75)**
  - **statistics** -- Reset link-keepalive counters for all UDLD enabled ports. **(p. 75)**
- clear **logging** -- Remove all event entries from the event log. **(p. 75)**
- clear **statistics** -- Reset all counters for the specified ports. ([ethernet] PORT-LIST) **(p. 75)**

COMMAND DETAILS

arp (p. 74)
client-public-key (p. 74)
crypto (p. 74)
intrusion-flags (p. 74)
ipv6 (p. 74)
keyfile (p. 74)
keylist (p. 74)
link-keepalive (p. 75)
logging (p. 75)
neighbors (p. 75)
statistics (p. 75)

arp

- clear arp

```
Flush all non-permanent entries in the ARP cache.
```

client-public-key

- clear crypto client-public-key

```
Remove client public keys from active configuration.
```

Next Available Option:

- **keyfile** < manager | operator > -- Remove client public keys from active configuration.**(p. 74)**

crypto

- clear crypto

```
Remove client public keys from active configuration.
```

Next Available Option:

- **client-public-key** -- Remove client public keys from active configuration.**(p. 74)**

intrusion-flags

- clear intrusion-flags

```
Reset the Alert Flag on all ports.
```

ipv6

- clear ipv6

```
Clear all IPv6 information.
```

Next Available Option:

- **neighbors** -- Delete all the neighbour discovery cache entries, except static entries.**(p. 75)**

keyfile

- clear crypto client-public-key *< manager | operator >*

```
Remove client public keys from active configuration.
```

Supported Values:

- **manager** -- Select manager public keys.
- **operator** -- Select operator public keys.

Next Available Option:

- **keylist** -- Remove client public keys from active configuration. (ASCII-STR) **(p. 74)**

keylist

- clear crypto client-public-key *< manager | operator > KEYLIST*

`Remove client public keys from active configuration.`

link-keepalive

- clear link-keepalive

  `Reset link-keepalive counters for all UDLD enabled ports.`

  Next Available Option:

  - **statistics** -- Reset link-keepalive counters for all UDLD enabled ports.**(p. 75)**

logging

- clear logging

  `Remove all event entries from the event log.`

neighbors

- clear ipv6 neighbors

  `Delete all the neighbour discovery cache entries, except static entries.`

statistics

- clear statistics *[ETHERNET] PORT-LIST*

  `Reset all counters for the specified ports.`

- clear link-keepalive statistics

  `Reset link-keepalive counters for all UDLD enabled ports.`

clock

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**ip (page 269)** **sntp (page 547)** **time (page 594)**

```
Usage: [no] clock [...]

Description: Display/set current time, date, and local time parameters.
             Called without any parameters displays the information
             mentioned above. Use 'clock ?' to see a list of all possible
             configuration options.
```

COMMAND STRUCTURE

- clock **set** -- Set current time and/or date **(p. 77)**
  - **date** -- Current date to set. (MM/DD[/[YY]YY]) **(p. 76)**
  - **time** -- Current time to set. (HH:MM[:SS]) **(p. 78)**
- [no] clock **summer-time** -- Enable/disable daylight-saving time changes **(p. 77)**
- clock **timezone** -- Set the number of hours your location is to the West(-) or East(+) of GMT **(p. 78)**
  - **gmt < +14:00 | +13:00 | +12:00 | ... >** -- Number of hours your timezone is to the West(-) or East(+) of GMT. **(p. 76)**
  - **us < alaska | aleutian | arizona | ... >** -- Timezone for US locations. **(p. 78)**

COMMAND DETAILS

date (p. 76)
gmt (p. 76)
set (p. 77)
summer-time (p. 77)
time (p. 78)
timezone (p. 78)
us (p. 78)

date

- clock set *[DATE]*

```
Current date to set.
```

gmt

- clock timezone gmt *< +14:00 | +13:00 | +12:00 | ... >*

```
Number of hours your timezone is to the West(-) or East(+) of GMT.
```

Supported Values:

- **+14:00**
- **+13:00**
- **+12:00**
- **+11:30**
- **+11:00**
- **+10:30**
- **+10:00**

- **+9:30**
- **+9:00**
- **+8:00**
- **+7:00**
- **+6:30**
- **+6:00**
- **+5:30**
- **+5:00**
- **+4:30**
- **+4:00**
- **+3:30**
- **+3:00**
- **+2:00**
- **+1:00**
- **+0:00**
- **-1:00**
- **-2:00**
- **-3:00**
- **-3:30**
- **-4:00**
- **-5:00**
- **-6:00**
- **-7:00**
- **-8:00**
- **-8:30**
- **-9:00**
- **-9:30**
- **-10:00**
- **-11:00**
- **-12:00**

set

- clock set

```
Usage: clock set <[MM/DD[/[YY]YY]] [HH:MM[:SS]]>

Description: Set current time and/or date.
             o MM/DD[/[YY]YY]    - New date
             o HH:MM[:SS]        - New time
```

Next Available Options:

- **date** -- Current date to set. (MM/DD[/[YY]YY]) **(p. 76)**
- **time** -- Current time to set. (HH:MM[:SS]) **(p. 78)**

summer-time

- [no] clock summer-time

```
Usage: [no] clock summer-time

Description: Enable/disable daylight-saving time changes.
```

time

- clock set *[TIME]*

```
Current time to set.
```

timezone

- clock timezone

```
Usage: clock timezone [gmt <-12:00 - +14:00>] |
                      [us  <none|alaska|aleutian|arizona|central|
                            east-indiana|eastern|hawaii|michigan|mountain|
                            pacific|samoa>]

Description: Set the number of hours your location is to the
             West(-) or East(+) of GMT. The number of hours can
             be defined by specifying either an exact number
             (see 'clock timezone gmt ?' for the list of all acceptable
             values) or a US timezone. The default value is GMT 0.
```

Next Available Options:

- **gmt** < +14:00 | +13:00 | +12:00 | ... > -- Number of hours your timezone is to the West(-) or East(+) of GMT.**(p. 76)**
- **us** < alaska | aleutian | arizona | ... > -- Timezone for US locations.**(p. 78)**

us

- clock timezone us *< alaska | aleutian | arizona | ... >*

```
Timezone for US locations.
```

Supported Values:

- **alaska**
- **aleutian**
- **arizona**
- **central**
- **east_indiana**
- **eastern**
- **hawaii**
- **michigan**
- **mountain**
- **pacific**
- **samoa**

configure

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**end (page 165)** **exit (page 168)** **enable (page 164)**

```
Usage: configure [terminal]

Description: Enter the Configuration context.
```

COMMAND STRUCTURE

- configure **terminal** -- Optional keyword of the configure command. Can be omitted. **(p. 79)**

EXAMPLES

Example: enable

```
ProCurve# configure
ProCurve(config)#
```

COMMAND DETAILS

terminal (p. 79)

terminal

- configure terminal

  Optional keyword of the configure command. Can be omitted.

connection-rate-filter

OVERVIEW

Category:	Troubleshooting
Primary context:	config
Related Commands	**filter (page 172)** **ip (page 269)** **vlan (page 611)** **show connection-rate-filter (page 465)**

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK >
       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Re-enables access to a host or set of hosts  that has been previously
             blocked by the connection rate filter. Disabling or setting sensitivity
             may have improved performance after rebooting the switch
```

COMMAND STRUCTURE

- connection-rate-filter **sensitivity** -- Sets the level of filtering required **(p. 81)**
  - **sensitive < low | medium | high | ... >** -- **(p. 80)**
- connection-rate-filter **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 81)**
  - **all** -- Resets all previously blocked by the connection rate filter **(p. 80)**
  - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 80)**
  - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 81)**

COMMAND DETAILS

all (p. 80)	**sensitive (p. 80)**	**src-ip (p. 81)**
host (p. 80)	**sensitivity (p. 81)**	**unblock (p. 81)**

all

- connection-rate-filter unblock all

```
Resets all previously blocked by the connection rate filter
```

host

- connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

sensitive

- connection-rate-filter sensitivity *< low | medium | high | ... >*

Supported Values:

- **low** -- Sets the level of connection rate filtering to low (most permissive)
- **medium** -- Sets the level of connection rate filtering to medium (permissive)
- **high** -- Sets the level of connection rate filtering to high (restrictive)
- **aggressive** -- Sets the level of connection rate filtering to aggressive (most restrictive)

sensitivity

- connection-rate-filter sensitivity

```
Sets the level of filtering required
```

Next Available Option:

- **sensitive** < low | medium | high | ... > -- **(p. 80)**

src-ip

- connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

unblock

- connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 80)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 80)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 81)**

console

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show (page 437)** **repeat (page 406)**

```
Usage: console ...

Description: Set various console parameters. Use 'console ?' to get a list
             of all configurable parameters.
             The non-configurable parameters and their default values are:
             Data bits = 8; Parity = None; Stop bits = 1.
```

COMMAND STRUCTURE

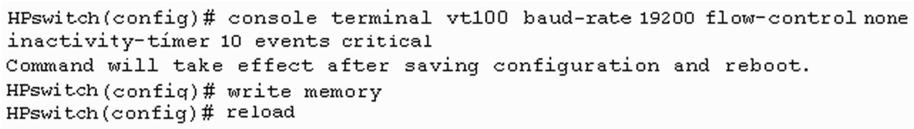
- console **baud-rate** **< speed-sense | 1200 | 2400 | ... >** -- Set the data transmission speed for the device connect sessions initiated through the Console port **(p. 83)**
- console **events** **< None | Debug | All | ... >** -- Set level of the events displayed in the device's Events Log **(p. 83)**
- console **flow-control** **< XON/XOFF | None >** -- Set the Flow Control Method; default is xon-xoff **(p. 83)**
- console **inactivity-timer** **< 0 | 1 | 5 | ... >** -- Set the number of minutes of no activity detected on the Console port before the switch terminates a communication session **(p. 84)**
- console **local-terminal** **< VT100 | NONE | ANSI >** -- Set type of terminal being used for the current console or telnet session (default is vt100) **(p. 84)**
- console **screen-refresh** **< 1 | 3 | 5 | ... >** -- Set default number of seconds before screen is refreshed on the repeat command **(p. 84)**
- console **terminal** **< VT100 | NONE | ANSI >** -- Set type of terminal being used for all console and telnet sessions (default is vt100) **(p. 85)**

EXAMPLES

Example: console <...>

Configure the switch to use the following console settings:

- VT100 operation
- 19,200 baud
- No flow control
- 10-minute inactivity time
- Critical log events



```
HPswitch(config)# console terminal vt100 baud-rate 19200 flow-control none
inactivity-timer 10 events critical
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# reload
```

COMMAND DETAILS

- baud-rate (p. 83)
- events (p. 83)
- flow-control (p. 83)
- inactivity-timer (p. 84)
- local-terminal (p. 84)
- screen-refresh (p. 84)
- terminal (p. 85)

baud-rate

- console baud-rate *< speed-sense | 1200 | 2400 | ... >*

```
Usage: console baud-rate <speed-sense|1200|2400|4800|
                          9600|19200|38400|57600|115200>

Description: Set the data transmission speed for the device connect
             sessions initiated through the Console port. The 'speed-sense'
             is for automatic speed determination. Default is speed-sense.
```

Supported Values:

- **speed-sense**
- **1200**
- **2400**
- **4800**
- **9600**
- **19200**
- **38400**
- **57600**
- **115200**

events

- console events *< None | Debug | All | ... >*

```
Usage: console events <none|all|not-info|critical|debug>

Description: Set level of the events displayed in the device's Events Log.
             all - display all;
             none - display no events;
             not-info - display all events except informational;
             critical - display only critical-level events;
             debug - reserved for Internal use.
```

Supported Values:

- **None**
- **Debug**
- **All**
- **Not-INFO**
- **Critical**

flow-control

- console flow-control *< XON/XOFF | None >*

```
Usage: console flow-control <xon/xoff|none>

Description: Set the Flow Control Method; default is xon-xoff.
```

Supported Values:

- **XON/XOFF**
- **None**

inactivity-timer

- console inactivity-timer *< 0 | 1 | 5 | ... >*

```
Usage: console inactivity-timer <0|1|5|10|15|20|30|60|120>

Description: Set the number of minutes of no activity detected on the
             Console port before the switch terminates a communication
             session. '0' means disable inactivity timer.
             Default is 0.
```

Supported Values:

- **0**
- **1**
- **5**
- **10**
- **15**
- **20**
- **30**
- **60**
- **120**

local-terminal

- console local-terminal *< VT100 | NONE | ANSI >*

```
Usage: console local-terminal <vt100|ansi|none>

Description: Set type of terminal being used for the current
             console or telnet session (default is vt100).
             Takes effect immediately. Not saved in configuration.

             Terminal type options are:
             vt100 = use VT100 terminal escape sequences.
             ansi = use ANSI terminal escape sequences.
             none = use a raw mode with no terminal escape sequences. Useful
             for scripting.

             See also 'console terminal help'.
```

Supported Values:

- **VT100** -- VT-100 terminal compatible.
- **NONE** -- Raw mode with terminal escape sequences removed.
- **ANSI** -- ANSI terminal compatible.

screen-refresh

- console screen-refresh *< 1 | 3 | 5 | ... >*

```
Usage: console screen-refresh <1|3|5|10|20|30|45|60>

Description: Set default number of seconds before screen is refreshed
```

```
             on the repeat command. See 'repeat help' for details on
             the 'repeat' command.
```

Supported Values:

- **1**
- **3**
- **5**
- **10**
- **20**
- **30**
- **45**
- **60**

terminal

- console terminal *< VT100 | NONE | ANSI >*

```
Usage: console terminal <vt100|ansi|none>

Description: Set type of terminal being used for all console
             and telnet sessions (default is vt100).  Saved in
             configuration and requires reboot to take effect.

             Terminal type options are:
             vt100 = use VT100 terminal escape sequences.
             ansi = use ANSI terminal escape sequences.
             none = use a raw mode with no terminal escape sequences. Useful
             for scripting.

             See also 'console local-terminal help'.
```

Supported Values:

- **VT100** -- VT-100 terminal compatible.
- **NONE** -- Raw mode with terminal escape sequences removed.
- **ANSI** -- ANSI terminal compatible.

copy

OVERVIEW

Category:	File Transfer
Primary context:	manager
Related Commands	**show config (page 462)** **show files (page 471)** **show flash (page 472)** **show running-config (page 506)**

```
Usage: copy <source> <destination> [options]

Description: Copy datafiles to/from the switch.

   <source> - specify source of data. It can be 'tftp', 'xmodem', 'command',
             'usb' or any of the following switch data files:
             o running-config
             o startup-config
             o crash-log [a|b|c|d|e|f|g|h|master]
             o crash-data
             o event-log
             o command-output <command>

       Note: When using 'command-output', place the desired CLI command in
             double-quotes. i.e. "show system".

   <destination> - specify the copy target. It can be also 'tftp', 'xmodem',
            'usb' or one of the following switch data files:
             o startup-config
             o command-file
             o flash
             o pub-key-file
             o autorun-key-file

   [options] - options are:
             o IPv4 address - TFTP server IPv4 address.
                              Required for TFTP transfers.
             o IPv6 address - TFTP server IPv6 address.
                              Required for TFTP transfers.
             o filename  - File-name to upload/download.
                            Required for TFTP & USB transfers.
             o unix
             o pc
```

COMMAND STRUCTURE

- copy **command-output** -- Specify a CLI command to copy output of. (ASCII-STR) **(p. 101)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
- copy **config < config | new >** -- Copy named configuration file. **(p. 101)**
  - **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 101)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
- copy **crash-data** -- Copy the switch crash data file. **(p. 101)**
  - **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 100)**
    - **tftp** -- Copy data to a TFTP server. **(p. 122)**
      - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **usb** -- Copy data to a USB flash drive. **(p. 131)**
      - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
        - **append** -- Add the key(s) for operator access. **(p. 94)**
        - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
          - **append** -- Add the key(s) for access. **(p. 94)**
        - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
          - **append** -- Add the key(s) for access. **(p. 94)**
    - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
  - **mm** -- Copy from the management card. **(p. 116)**
    - **tftp** -- Copy data to a TFTP server. **(p. 122)**
      - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **usb** -- Copy data to a USB flash drive. **(p. 131)**
      - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

        - **append** -- Add the key(s) for operator access. **(p. 94)**
        - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
          - **append** -- Add the key(s) for access. **(p. 94)**
        - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
          - **append** -- Add the key(s) for access. **(p. 94)**
    - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
- copy **crash-log** -- Copy the switch log file. **(p. 102)**
  - **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 100)**
    - **tftp** -- Copy data to a TFTP server. **(p. 122)**
      - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **usb** -- Copy data to a USB flash drive. **(p. 131)**
      - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
        - **append** -- Add the key(s) for operator access. **(p. 94)**
        - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
          - **append** -- Add the key(s) for access. **(p. 94)**
        - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
          - **append** -- Add the key(s) for access. **(p. 94)**
    - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
  - **mm** -- Copy from the management card. **(p. 116)**
    - **tftp** -- Copy data to a TFTP server. **(p. 122)**
      - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
        - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **usb** -- Copy data to a USB flash drive. **(p. 131)**
      - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
        - **append** -- Add the key(s) for operator access. **(p. 94)**
        - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
          - **append** -- Add the key(s) for access. **(p. 94)**

        - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
          - **append** -- Add the key(s) for access. **(p. 94)**
    - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
- copy **event-log** -- Copy event log file. **(p. 103)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
- copy **flash** -- Copy the switch system image file. **(p. 111)**
  - **flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 111)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**

        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
- copy **running-config** -- Copy running configuration file. **(p. 121)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
- copy **startup-config** -- Copy in-flash configuration file. **(p. 121)**
  - **tftp** -- Copy data to a TFTP server. **(p. 122)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **usb** -- Copy data to a USB flash drive. **(p. 131)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 133)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
- copy **tftp** -- Copy data from a TFTP server. **(p. 122)**
  - **autorun-cert-file** -- Copy autorun trusted certificate to the switch. **(p. 99)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
- **autorun-key-file** -- Copy autorun key file to the switch. **(p. 99)**
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
- **command-file** -- Copy command script to switch and execute. **(p. 100)**
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **pc** -- Change CR/LF to PC style. **(p. 119)**
      - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **pc** -- Change CR/LF to PC style. **(p. 119)**
      - **unix** -- Change CR/LF to unix style. **(p. 130)**
- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 101)**
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **pc** -- Change CR/LF to PC style. **(p. 119)**
      - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
      - **pc** -- Change CR/LF to PC style. **(p. 119)**
      - **unix** -- Change CR/LF to unix style. **(p. 130)**

  - **flash** -- Copy data to the switch system image file. **(p. 111)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 102)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 102)**
  - **pub-key-file** -- Copy the public keys to the switch. **(p. 121)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **append** -- Add the key(s) for operator access. **(p. 94)**
        - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
          - **append** -- Add the key(s) for access. **(p. 94)**
        - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
          - **append** -- Add the key(s) for access. **(p. 94)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **append** -- Add the key(s) for operator access. **(p. 94)**
        - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
          - **append** -- Add the key(s) for access. **(p. 94)**
        - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
          - **append** -- Add the key(s) for access. **(p. 94)**
  - **startup-config** -- Copy data to the switch configuration file. **(p. 121)**
    - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
    - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**
        - **pc** -- Change CR/LF to PC style. **(p. 119)**
        - **unix** -- Change CR/LF to unix style. **(p. 130)**
- copy **usb** -- Copy data from a USB flash drive. **(p. 131)**
  - **autorun-cert-file** -- Copy autorun trusted certificate to the switch. **(p. 99)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **autorun-key-file** -- Copy autorun key file to the switch. **(p. 99)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**

        - **append** -- Add the key(s) for access. **(p. 94)**
  - **command-file** -- Copy command script to switch and execute. **(p. 100)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **pc** -- Change CR/LF to PC style. **(p. 119)**
      - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **flash** -- Copy data to the switch system image file. **(p. 111)**
    - **image-name** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 112)**
      - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 102)**
  - **pub-key-file** -- Copy the public keys to the switch. **(p. 121)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
  - **startup-config** -- Copy data to the switch configuration file. **(p. 121)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**
      - **append** -- Add the key(s) for operator access. **(p. 94)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 112)**
        - **append** -- Add the key(s) for access. **(p. 94)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 116)**
        - **append** -- Add the key(s) for access. **(p. 94)**
- copy **xmodem** -- Use xmodem on the terminal as the data source. **(p. 133)**
  - **command-file** -- Copy command script to switch and execute. **(p. 100)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 101)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**
  - **flash** -- Copy to primary/secondary flash. **(p. 111)**
    - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 102)**
  - **startup-config** -- Copy data to the switch configuration file. **(p. 121)**
    - **pc** -- Change CR/LF to PC style. **(p. 119)**
    - **unix** -- Change CR/LF to unix style. **(p. 130)**

EXAMPLES

Example: copy config tftp

Copy a startup-config file named test-01 from the switch to a UNIX TFTP server at IP address 10.10.28.14:

```
ProCurve(config)# copy config test-01 tftp 10.10.28.14 test-01.txt unix
```

Example: copy flash flash primary

Copy the image in secondary flash to primary flash:

```
ProCurve(config)# copy flash flash primary
```

COMMAND DETAILS

append

- copy tftp pub-key-file *IP-ADDR FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy tftp pub-key-file *IP-ADDR FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy tftp pub-key-file *IP-ADDR FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy tftp pub-key-file *IPV6-ADDR FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy tftp pub-key-file *IPV6-ADDR FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy tftp pub-key-file *IPV6-ADDR FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-cert-file *IP-ADDR FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy tftp autorun-cert-file *IP-ADDR FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-cert-file *IP-ADDR FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-cert-file *IPV6-ADDR FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy tftp autorun-cert-file *IPV6-ADDR FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-cert-file *IPV6-ADDR FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-key-file *IP-ADDR FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy tftp autorun-key-file *IP-ADDR FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-key-file *IP-ADDR FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-key-file *IPV6-ADDR FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy tftp autorun-key-file *IPV6-ADDR FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy tftp autorun-key-file *IPV6-ADDR FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy usb startup-config *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy usb startup-config *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy usb startup-config *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy usb pub-key-file *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy usb pub-key-file *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy usb pub-key-file *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy usb autorun-cert-file *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy usb autorun-cert-file *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy usb autorun-cert-file *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy usb autorun-key-file *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy usb autorun-key-file *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy usb autorun-key-file *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy command-output *COMMAND-OUTPUT* usb *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy command-output *COMMAND-OUTPUT* usb *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy command-output *COMMAND-OUTPUT* usb *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy crash-data mm usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy crash-data mm usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy crash-data mm usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy crash-data usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy crash-data usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy crash-data usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy crash-log mm usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy crash-log mm usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy crash-log mm usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy crash-log usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy crash-log usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy crash-log usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy flash usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy flash usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy flash usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy running-config usb *FILENAME* append

  `Add the key(s) for operator access.`

- copy running-config usb *FILENAME* operator append

  `Add the key(s) for access.`

- copy running-config usb *FILENAME* manager append

  `Add the key(s) for access.`

- copy startup-config usb *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy startup-config usb *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy startup-config usb *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

- copy event-log usb *FILENAME* append

  ```
  Add the key(s) for operator access.
  ```

- copy event-log usb *FILENAME* operator append

  ```
  Add the key(s) for access.
  ```

- copy event-log usb *FILENAME* manager append

  ```
  Add the key(s) for access.
  ```

autorun-cert-file

- copy tftp autorun-cert-file

  ```
  Copy autorun trusted certificate to the switch.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy usb autorun-cert-file

  ```
  Copy autorun trusted certificate to the switch.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

autorun-key-file

- copy tftp autorun-key-file

  ```
  Copy autorun key file to the switch.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy usb autorun-key-file

  `Copy autorun key file to the switch.`

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

card

- copy crash-data *SLOT-ID-RANGE*

  `Enter single slot identifier.`

  Next Available Options:
  - **tftp** -- Copy data to a TFTP server.**(p. 122)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
  - **usb** -- Copy data to a USB flash drive.**(p. 131)**

- copy crash-log *SLOT-ID-RANGE*

  `Enter single slot identifier.`

  Next Available Options:
  - **tftp** -- Copy data to a TFTP server.**(p. 122)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
  - **usb** -- Copy data to a USB flash drive.**(p. 131)**

command-file

- copy tftp command-file

  `Copy command script to switch and execute.`

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy xmodem command-file

  `Copy command script to switch and execute.`

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy usb command-file

  `Copy command script to switch and execute.`

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

command-output

- copy command-output *COMMAND-OUTPUT*

  ```
  Specify a CLI command to copy output of.
  ```

  Next Available Options:
  - **tftp** -- Copy data to a TFTP server.**(p. 122)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
  - **usb** -- Copy data to a USB flash drive.**(p. 131)**

config

- copy tftp config *CONFIG*

  ```
  Copy data to specified configuration file.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy xmodem config *CONFIG*

  ```
  Copy data to specified configuration file.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy config *< config | new >*

  ```
  Copy named configuration file.
  ```

  Supported Values:
  - **config**
  - **new**

  Next Available Options:
  - **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 101)**
  - **tftp** -- Copy data to a TFTP server.**(p. 122)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**

- copy config *< config | new >* config *CONFIG*

  ```
  Copy data to specified configuration file.
  ```

crash-data

- copy crash-data

  ```
  Copy the switch crash data file.
  ```

Next Available Options:

- **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 100)**
- **mm** -- Copy from the management card.**(p. 116)**
- **tftp** -- Copy data to a TFTP server.**(p. 122)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
- **usb** -- Copy data to a USB flash drive.**(p. 131)**

crash-log

- copy crash-log

```
Copy the switch log file.
```

Next Available Options:

- **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 100)**
- **mm** -- Copy from the management card.**(p. 116)**
- **tftp** -- Copy data to a TFTP server.**(p. 122)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
- **usb** -- Copy data to a USB flash drive.**(p. 131)**

cv_flash

- copy tftp flash *IP-ADDR FILENAME* < *primary* | *secondary* >

```
Copy to primary/secondary flash.
```

Supported Values:

- **primary** -- Copy to primary flash.
- **secondary** -- Copy to secondary flash.

- copy tftp flash *IPV6-ADDR FILENAME* < *primary* | *secondary* >

```
Copy to primary/secondary flash.
```

Supported Values:

- **primary** -- Copy to primary flash.
- **secondary** -- Copy to secondary flash.

- copy xmodem flash < *primary* | *secondary* >

```
Copy to primary/secondary flash.
```

Supported Values:

- **primary** -- Copy to primary flash.
- **secondary** -- Copy to secondary flash.

- copy usb flash *IMAGE-NAME* < *primary* | *secondary* >

```
Copy to primary/secondary flash.
```

Supported Values:

- **primary** -- Copy to primary flash.

- **secondary** -- Copy to secondary flash.

event-log

- copy event-log

```
Copy event log file.
```

Next Available Options:

- **tftp** -- Copy data to a TFTP server.**(p. 122)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
- **usb** -- Copy data to a USB flash drive.**(p. 131)**

filename

- copy tftp command-file *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy tftp command-file *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy tftp flash *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:

- **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 102)**

- copy tftp flash *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:

- **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 102)**

- copy tftp pub-key-file *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**

  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy tftp pub-key-file *IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy tftp startup-config *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy tftp startup-config *IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy tftp config *CONFIG IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy tftp config *CONFIG IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy tftp autorun-cert-file *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy tftp autorun-cert-file *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy tftp autorun-key-file *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy tftp autorun-key-file *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy usb startup-config *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy usb command-file *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy usb pub-key-file *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:
  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy usb autorun-cert-file *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:
  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy usb autorun-key-file *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:
  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy command-output *COMMAND-OUTPUT* tftp *IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy command-output *COMMAND-OUTPUT* usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy config *< config | new >* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy config *< config | new >* tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy crash-data *SLOT-ID-RANGE* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-data *SLOT-ID-RANGE* tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy crash-data mm tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-data mm tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-data mm usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy crash-data tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-data tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-data usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy crash-log *SLOT-ID-RANGE* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-log *SLOT-ID-RANGE* tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy crash-log mm tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-log mm tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-log mm usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy crash-log tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-log tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy crash-log usb *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:

- **append** -- Add the key(s) for operator access.**(p. 94)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy flash tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy flash tftp *IPV6-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

- copy flash usb *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:
  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy running-config tftp *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy running-config tftp *IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy running-config usb *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:
  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy startup-config tftp *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy startup-config tftp *IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy startup-config usb *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:

  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

- copy event-log tftp *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:

  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy event-log tftp *IPV6-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:

  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy event-log usb *FILENAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Options:

  - **append** -- Add the key(s) for operator access.**(p. 94)**
  - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 116)**
  - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 112)**

flash

- copy tftp flash

  ```
  Copy data to the switch system image file.
  ```

  Next Available Options:

  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy xmodem flash

  ```
  Copy to primary/secondary flash.
  ```

  Next Available Option:
  - **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 102)**

- copy usb flash

  ```
  Copy data to the switch system image file.
  ```

  Next Available Option:
  - **image-name** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 112)**

- copy flash

  ```
  Copy the switch system image file.
  ```

  Next Available Options:
  - **flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 111)**
  - **tftp** -- Copy data to a TFTP server.**(p. 122)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
  - **usb** -- Copy data to a USB flash drive.**(p. 131)**

- copy flash flash *< primary | secondary >*

  ```
  Copy to primary/secondary flash.
  ```

  Supported Values:
  - **primary** -- Copy to primary flash.
  - **secondary** -- Copy to secondary flash.

image-name

- copy usb flash *IMAGE-NAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Option:
  - **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 102)**

manager

- copy tftp pub-key-file *IP-ADDR FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp pub-key-file *IPV6-ADDR FILENAME* manager

```
Replace the key(s) for manager access; follow with the 'append' option to add the
key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-cert-file *IP-ADDR FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-cert-file *IPV6-ADDR FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-key-file *IP-ADDR FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-key-file *IPV6-ADDR FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy usb startup-config *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy usb pub-key-file *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy usb autorun-cert-file *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy usb autorun-key-file *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy command-output *COMMAND-OUTPUT* usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-data mm usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-data usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:

  - **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-log mm usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-log usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy flash usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy running-config usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy startup-config usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy event-log usb *FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

mm

- copy crash-data mm

```
Copy from the management card.
```

Next Available Options:

- **tftp** -- Copy data to a TFTP server.**(p. 122)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
- **usb** -- Copy data to a USB flash drive.**(p. 131)**

- copy crash-log mm

```
Copy from the management card.
```

Next Available Options:

- **tftp** -- Copy data to a TFTP server.**(p. 122)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
- **usb** -- Copy data to a USB flash drive.**(p. 131)**

operator

- copy tftp pub-key-file *IP-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp pub-key-file *IPV6-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-cert-file *IP-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-cert-file *IPV6-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-key-file *IP-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy tftp autorun-key-file *IPV6-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy usb startup-config *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy usb pub-key-file *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy usb autorun-cert-file *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy usb autorun-key-file *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy command-output *COMMAND-OUTPUT* usb *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-data mm usb *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-data usb *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-log mm usb *FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Option:

- **append** -- Add the key(s) for access.**(p. 94)**

- copy crash-log usb *FILENAME* operator

  ```
  Replace the key(s) for operator access (default); follow with the 'append' option to
   add the key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy flash usb *FILENAME* operator

  ```
  Replace the key(s) for operator access (default); follow with the 'append' option to
   add the key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy running-config usb *FILENAME* operator

  ```
  Replace the key(s) for operator access (default); follow with the 'append' option to
   add the key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy startup-config usb *FILENAME* operator

  ```
  Replace the key(s) for operator access (default); follow with the 'append' option to
   add the key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

- copy event-log usb *FILENAME* operator

  ```
  Replace the key(s) for operator access (default); follow with the 'append' option to
   add the key(s).
  ```

  Next Available Option:
  - **append** -- Add the key(s) for access.**(p. 94)**

pc

- copy tftp command-file *IP-ADDR FILENAME* pc

  ```
  Change CR/LF to PC style.
  ```

- copy tftp command-file *IPV6-ADDR FILENAME* pc

  ```
  Change CR/LF to PC style.
  ```

- copy tftp startup-config *IP-ADDR FILENAME* pc

  ```
  Change CR/LF to PC style.
  ```

- copy tftp startup-config *IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy tftp config *CONFIG IP-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy tftp config *CONFIG IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy xmodem startup-config pc

  `Change CR/LF to PC style.`

- copy xmodem command-file pc

  `Change CR/LF to PC style.`

- copy xmodem config *CONFIG* pc

  `Change CR/LF to PC style.`

- copy usb command-file *FILENAME* pc

  `Change CR/LF to PC style.`

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy command-output *COMMAND-OUTPUT* tftp *IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy command-output *COMMAND-OUTPUT* xmodem pc

  `Change CR/LF to PC style.`

- copy config < *config* | *new* > tftp *IP-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy config < *config* | *new* > tftp *IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy config < *config* | *new* > xmodem pc

  `Change CR/LF to PC style.`

- copy running-config tftp *IP-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy running-config tftp *IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy running-config xmodem pc

  `Change CR/LF to PC style.`

- copy startup-config tftp *IP-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy startup-config tftp *IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy startup-config xmodem pc

  `Change CR/LF to PC style.`

- copy event-log tftp *IP-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy event-log tftp *IPV6-ADDR FILENAME* pc

  `Change CR/LF to PC style.`

- copy event-log xmodem pc

  `Change CR/LF to PC style.`

pub-key-file

- copy tftp pub-key-file

  `Copy the public keys to the switch.`

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy usb pub-key-file

  `Copy the public keys to the switch.`

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

running-config

- copy running-config

  `Copy running configuration file.`

  Next Available Options:
  - **tftp** -- Copy data to a TFTP server.**(p. 122)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
  - **usb** -- Copy data to a USB flash drive.**(p. 131)**

startup-config

- copy tftp startup-config

  `Copy data to the switch configuration file.`

Next Available Options:

- **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
- **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy xmodem startup-config

```
Copy data to the switch configuration file.
```

Next Available Options:

- **unix** -- Change CR/LF to unix style.**(p. 130)**
- **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy usb startup-config

```
Copy data to the switch configuration file.
```

Next Available Option:

- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy startup-config

```
Copy in-flash configuration file.
```

Next Available Options:

- **tftp** -- Copy data to a TFTP server.**(p. 122)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 133)**
- **usb** -- Copy data to a USB flash drive.**(p. 131)**

tftp

- copy tftp

```
Copy data from a TFTP server.
```

Next Available Options:

- **command-file** -- Copy command script to switch and execute.**(p. 100)**
- **flash** -- Copy data to the switch system image file.**(p. 111)**
- **pub-key-file** -- Copy the public keys to the switch.**(p. 121)**
- **startup-config** -- Copy data to the switch configuration file.**(p. 121)**
- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 101)**
- **autorun-cert-file** -- Copy autorun trusted certificate to the switch.**(p. 99)**
- **autorun-key-file** -- Copy autorun key file to the switch.**(p. 99)**

- copy command-output *COMMAND-OUTPUT* tftp

```
Copy data to a TFTP server.
```

Next Available Options:

- **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
- **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy config *< config | new >* tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy crash-data *SLOT-ID-RANGE* tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy crash-data mm tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy crash-data tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy crash-log *SLOT-ID-RANGE* tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy crash-log mm tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy crash-log tftp

  ```
  Copy data to a TFTP server.
  ```

Next Available Options:
- **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
- **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy flash tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy running-config tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy startup-config tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

- copy event-log tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Options:
  - **tftp-ip** -- Specify TFTP server IPv4 address. (IP-ADDR) **(p. 124)**
  - **tftp-ipv6** -- Specify TFTP server IPv6 address. (IPV6-ADDR) **(p. 127)**

tftp-ip

- copy tftp command-file *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp flash *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp pub-key-file *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp startup-config *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp config *CONFIG IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp autorun-cert-file *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp autorun-key-file *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy config < *config* | *new* > tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-data *SLOT-ID-RANGE* tftp *IP-ADDR*

```
Specify TFTP server IPv4 address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-data mm tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-data tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-log *SLOT-ID-RANGE* tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-log mm tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-log tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy flash tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy running-config tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

Next Available Option:

- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy startup-config tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy event-log tftp *IP-ADDR*

  ```
  Specify TFTP server IPv4 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

tftp-ipv6

- copy tftp command-file *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp flash *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp pub-key-file *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp startup-config *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp config *CONFIG IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

Next Available Option:

- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp autorun-cert-file *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy tftp autorun-key-file *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy command-output *COMMAND-OUTPUT* tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy config *< config | new >* tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-data *SLOT-ID-RANGE* tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-data mm tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-data tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-log *SLOT-ID-RANGE* tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-log mm tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy crash-log tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy flash tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy running-config tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy startup-config tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

- copy event-log tftp *IPV6-ADDR*

  ```
  Specify TFTP server IPv6 address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 103)**

unix

- copy tftp command-file *IP-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy tftp command-file *IPV6-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy tftp startup-config *IP-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy tftp startup-config *IPV6-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy tftp config *CONFIG IP-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy tftp config *CONFIG IPV6-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy xmodem startup-config unix

  `Change CR/LF to unix style.`

- copy xmodem command-file unix

  `Change CR/LF to unix style.`

- copy xmodem config *CONFIG* unix

  `Change CR/LF to unix style.`

- copy usb command-file *FILENAME* unix

  `Change CR/LF to unix style.`

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy command-output *COMMAND-OUTPUT* tftp *IPV6-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy command-output *COMMAND-OUTPUT* xmodem unix

  `Change CR/LF to unix style.`

- copy config < *config* | *new* > tftp *IP-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy config < *config* | *new* > tftp *IPV6-ADDR FILENAME* unix

  `Change CR/LF to unix style.`

- copy config < *config* | *new* > xmodem unix

```
Change CR/LF to unix style.
```

- copy running-config tftp *IP-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy running-config tftp *IPV6-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy running-config xmodem unix

  ```
  Change CR/LF to unix style.
  ```

- copy startup-config tftp *IP-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy startup-config tftp *IPV6-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy startup-config xmodem unix

  ```
  Change CR/LF to unix style.
  ```

- copy event-log tftp *IP-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy event-log tftp *IPV6-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy event-log xmodem unix

  ```
  Change CR/LF to unix style.
  ```

usb

- copy usb

  ```
  Copy data from a USB flash drive.
  ```

  Next Available Options:
  - **startup-config** -- Copy data to the switch configuration file.**(p. 121)**
  - **flash** -- Copy data to the switch system image file.**(p. 111)**
  - **command-file** -- Copy command script to switch and execute.**(p. 100)**
  - **pub-key-file** -- Copy the public keys to the switch.**(p. 121)**
  - **autorun-cert-file** -- Copy autorun trusted certificate to the switch.**(p. 99)**
  - **autorun-key-file** -- Copy autorun key file to the switch.**(p. 99)**

- copy command-output *COMMAND-OUTPUT* usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy crash-data *SLOT-ID-RANGE* usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy crash-data mm usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy crash-data usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy crash-log *SLOT-ID-RANGE* usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy crash-log mm usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy crash-log usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy flash usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy running-config usb

```
Copy data to a USB flash drive.
```

Next Available Option:

- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy startup-config usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

- copy event-log usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:

  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 103)**

xmodem

- copy xmodem

  ```
  Use xmodem on the terminal as the data source.
  ```

  Next Available Options:

  - **flash** -- Copy to primary/secondary flash.**(p. 111)**
  - **startup-config** -- Copy data to the switch configuration file.**(p. 121)**
  - **command-file** -- Copy command script to switch and execute.**(p. 100)**
  - **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 101)**

- copy command-output *COMMAND-OUTPUT* xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:

  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy config < *config* | *new* > xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:

  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy crash-data *SLOT-ID-RANGE* xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy crash-data mm xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy crash-data xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy crash-log *SLOT-ID-RANGE* xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy crash-log mm xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy crash-log xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy flash xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

- copy running-config xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy startup-config xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

- copy event-log xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:
  - **unix** -- Change CR/LF to unix style.**(p. 130)**
  - **pc** -- Change CR/LF to PC style.**(p. 119)**

crypto

OVERVIEW

Category:	SSH
Primary context:	config
Related Commands	**the section called “crypto” (page 466)** **autorun (page 62)**

```
Usage: crypto host-cert generate self-signed [START END CNAME OU ORG
                                              CITY STATE COUNTRY]
       crypto host-cert zeroize
       crypto key generate <ssh [rsa] | cert [rsa] KEYSIZE | autorun-key [rsa]>
       crypto key zeroize <ssh | cert | autorun>

Description: Install or remove authentication files for ssh or https server
             or for autorun

Parameters:

    o host-cert - operation on the https host certificate file. The host
             certificate file cannot be created before the certificate
             rsa key file has been created.
    o key - operation on an ssh or https rsa key file.
    o generate - install new key or self-signed certificate.
             Note: installing a new key may be very slow in the first few
             minutes after booting the device.
    o zeroize - remove an existing key or certificate file.

    o self-signed - install new self-signed certificate.
    o START - certificate will be valid beginning on this date.
    o END - certificate will be valid until this date.
    o CNAME - the name (IP address) of this device.
    o OU - organizational unit or department.
    o ORG - organization name.
    o CITY - city or location.
    o STATE - state or region.
    o COUNTRY - two character ISO country code.  Typing 'x<TAB>' will
             provide a list of all valid country codes beginning with
             the letter x.

    o ssh - Install/remove host key for ssh server.
    o cert - Install/remove rsa key for https certificate.
    o autorun-key - Install/remove rsa key for autorun.
    o rsa - optional keyword indicating key type (only rsa is available).
    o KEYSIZE - for a certificate key, the size of the key desired.
             Certificate keys may be 512, 768, or 1024 bits.  (Ssh host
             keys are always 896 bits.)
```

COMMAND STRUCTURE

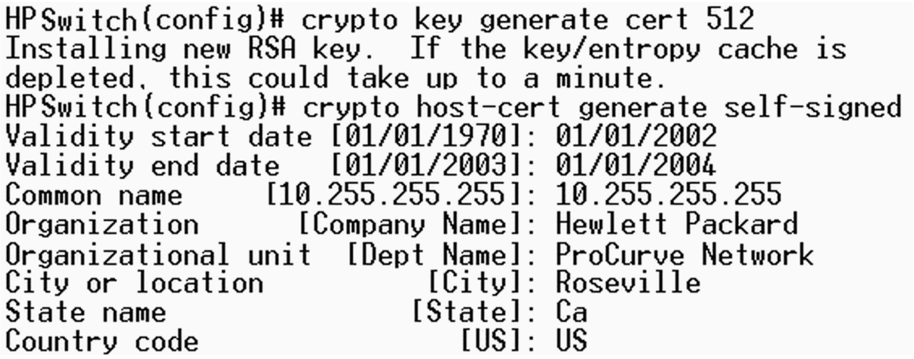
- crypto **host-cert** -- Install/remove self-signed certificate for https. **(p. 143)**
  - **generate** -- Create a self-signed certificate for the https server. **(p. 143)**
    - **self-signed** -- Create a self-signed certificate for the https server. **(p. 144)**
      - **start-date** -- Validity start date for certificate. (MM/DD[/[YY]YY]) **(p. 145)**
        - **end-date** -- Validity end date for certificate. (MM/DD[/[YY]YY]) **(p. 142)**

          - **cname** -- Common name [e.g., IP address of device]. (ASCII-STR) **(p. 137)**
            - **org-unit** -- Organizational unit [Department]. (ASCII-STR) **(p. 144)**
              - **organization** -- Organization name. (ASCII-STR) **(p. 144)**
                - *additional options available...*
  - **zeroize** -- Delete an existing certificate. **(p. 145)**
- crypto **key** -- Install/remove RSA key file for ssh or https server. **(p. 143)**
  - **generate** -- Generate a new key. **(p. 143)**
    - **autorun-key** -- Install RSA key file for autorun **(p. 137)**
      - **rsa** -- Optional keyword. **(p. 144)**
    - **cert** -- Install RSA key file for https certificate. **(p. 137)**
      - **key-size < 512 | 768 | 1024 >** -- **(p. 143)**
      - **rsa** -- Optional keyword. **(p. 144)**
        - **key-size < 512 | 768 | 1024 >** -- **(p. 143)**
    - **ssh** -- Install RSA key file for ssh server. **(p. 144)**
      - **rsa** -- Optional keyword. **(p. 144)**
  - **zeroize** -- Delete existing key. **(p. 145)**
    - **autorun** -- Remove RSA key file for autorun **(p. 136)**
      - **rsa** -- Optional keyword. **(p. 144)**
    - **cert** -- Remove RSA key file for https certificate. **(p. 137)**
    - **ssh** -- Remove RSA key file for ssh server. **(p. 144)**

EXAMPLES

Example: crypto key generate cert

Generate a key and a new host certificate:



```
HPSwitch(config)# crypto key generate cert 512
Installing new RSA key.  If the key/entropy cache is
depleted, this could take up to a minute.
HPSwitch(config)# crypto host-cert generate self-signed
Validity start date [01/01/1970]: 01/01/2002
Validity end date   [01/01/2003]: 01/01/2004
Common name      [10.255.255.255]: 10.255.255.255
Organization       [Company Name]: Hewlett Packard
Organizational unit   [Dept Name]: ProCurve Network
City or location           [City]: Roseville
State name                [State]: Ca
Country code                 [US]: US
```

COMMAND DETAILS

autorun (p. 136)
autorun-key (p. 137)
cert (p. 137)
city (p. 137)
cname (p. 137)
country (p. 137)
end-date (p. 142)
generate (p. 143)
host-cert (p. 143)
key (p. 143)
key-size (p. 143)
organization (p. 144)
org-unit (p. 144)
rsa (p. 144)
self-signed (p. 144)
ssh (p. 144)
start-date (p. 145)
state (p. 145)
zeroize (p. 145)

autorun

- crypto key zeroize autorun

```
Remove RSA key file for autorun
```

Next Available Option:

- **rsa** -- Optional keyword.**(p. 144)**

autorun-key

- crypto key generate autorun-key

```
Install RSA key file for autorun. The encryption key is a pre-requisite for
enabling autorun in secure-mode.
```

Next Available Option:

- **rsa** -- Optional keyword.**(p. 144)**

cert

- crypto key generate cert

```
Install RSA key file for https certificate.
```

Next Available Options:

- **rsa** -- Optional keyword.**(p. 144)**
- **key-size** < 512 | 768 | 1024 > -- **(p. 143)**

- crypto key zeroize cert

```
Remove RSA key file for https certificate.
```

city

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION CITY*

```
City or location.
```

Next Available Option:

- **state** -- State or region. (ASCII-STR) **(p. 145)**

cname

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME*

```
Common name [e.g., IP address of device].
```

Next Available Option:

- **org-unit** -- Organizational unit [Department]. (ASCII-STR) **(p. 144)**

country

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION CITY STATE < AD | AE | AF | ... >*

```
Country code (2 character ISO code).
```

Supported Values:

- **AD** -- Andorra

- **AE** -- United Arab Emirates
- **AF** -- Afghanistan
- **AG** -- Antigua and Barbuda
- **AI** -- Anguilla
- **AL** -- Albania
- **AM** -- Armenia
- **AN** -- Netherlands Antilles
- **AO** -- Angola
- **AQ** -- Antarctica
- **AR** -- Argentina
- **AS** -- American Samoa
- **AT** -- Austria
- **AU** -- Australia
- **AW** -- Aruba
- **AX** -- Aland Islands
- **AZ** -- Azerbaijan
- **BA** -- Bosnia and Herzegovina
- **BB** -- Barbados
- **BD** -- Bangladesh
- **BE** -- Belgium
- **BF** -- Burkina Faso
- **BG** -- Bulgaria
- **BH** -- Bahrain
- **BI** -- Burundi
- **BJ** -- Benin
- **BM** -- Bermuda
- **BN** -- Brunei Darussalam
- **BO** -- Bolivia
- **BR** -- Brazil
- **BS** -- Bahamas
- **BT** -- Bhutan
- **BV** -- Bouvet Island
- **BW** -- Botswana
- **BY** -- Belarus
- **BZ** -- Belize
- **CA** -- Canada
- **CC** -- Cocos (Keeling) Islands
- **CD** -- Congo, Democratic Republic of the
- **CF** -- Central African Republic
- **CG** -- Congo
- **CH** -- Switzerland
- **CI** -- Cote D'Ivoire (Ivory Coast)
- **CK** -- Cook Islands
- **CL** -- Chile
- **CM** -- Cameroon
- **CN** -- China
- **CO** -- Colombia
- **CR** -- Costa Rica
- **CS** -- Czechoslovakia (former)
- **CU** -- Cuba
- **CV** -- Cape Verde
- **CX** -- Christmas Island

- **CY** -- Cyprus
- **CZ** -- Czech Republic
- **DE** -- Germany
- **DJ** -- Djibouti
- **DK** -- Denmark
- **DM** -- Dominica
- **DO** -- Dominican Republic
- **DZ** -- Algeria
- **EC** -- Ecuador
- **EE** -- Estonia
- **EG** -- Egypt
- **EH** -- Western Sahara
- **ER** -- Eritrea
- **ES** -- Spain
- **ET** -- Ethiopia
- **FI** -- Finland
- **FJ** -- Fiji
- **FK** -- Falkland Islands (Malvinas)
- **FM** -- Micronesia
- **FO** -- Faroe Islands
- **FR** -- France
- **FX** -- France, Metropolitan
- **GA** -- Gabon
- **GB** -- Great Britain (UK)
- **GD** -- Grenada
- **GE** -- Georgia
- **GF** -- French Guiana
- **GG** -- Guernsey
- **GH** -- Ghana
- **GI** -- Gibraltar
- **GL** -- Greenland
- **GM** -- Gambia
- **GN** -- Guinea
- **GP** -- Guadeloupe
- **GQ** -- Equatorial Guinea
- **GR** -- Greece
- **GS** -- S. Georgia and S. Sandwich Isls.
- **GT** -- Guatemala
- **GU** -- Guam
- **GW** -- Guinea-Bissau
- **GY** -- Guyanav
- **HK** -- Hong Kong
- **HM** -- Heard and McDonald Islands
- **HN** -- Honduras
- **HR** -- Croatia (Hrvatska)
- **HT** -- Haiti
- **HU** -- Hungary
- **ID** -- Indonesia
- **IE** -- Ireland
- **IL** -- Israel
- **IM** -- Isle of Man
- **IN** -- India

- **IO** -- British Indian Ocean Territory
- **IQ** -- Iraq
- **IR** -- Iran
- **IS** -- Iceland
- **IT** -- Italy
- **JE** -- Jersey
- **JM** -- Jamaica
- **JO** -- Jordan
- **JP** -- Japan
- **KE** -- Kenya
- **KG** -- Kyrgyzstan
- **KH** -- Cambodia
- **KI** -- Kiribati
- **KM** -- Comoros
- **KN** -- Saint Kitts and Nevis
- **KP** -- Korea (North)
- **KR** -- Korea (South)
- **KW** -- Kuwait
- **KY** -- Cayman Islands
- **KZ** -- Kazakhstan
- **LA** -- Laos
- **LB** -- Lebanon
- **LC** -- Saint Lucia
- **LI** -- Liechtenstein
- **LK** -- Sri Lanka
- **LR** -- Liberia
- **LS** -- Lesotho
- **LT** -- Lithuania
- **LU** -- Luxembourg
- **LV** -- Latvia
- **LY** -- Libya
- **MA** -- Morocco
- **MC** -- Monaco
- **MD** -- Moldova
- **ME** -- Montenegro
- **MG** -- Madagascar
- **MH** -- Marshall Islands
- **MK** -- Macedonia
- **ML** -- Mali
- **MM** -- Myanmar
- **MN** -- Mongolia
- **MO** -- Macau
- **MP** -- Northern Mariana Islands
- **MQ** -- Martinique
- **MR** -- Mauritania
- **MS** -- Montserrat
- **MT** -- Malta
- **MU** -- Mauritius
- **MV** -- Maldives
- **MW** -- Malawi
- **MX** -- Mexico
- **MY** -- Malaysia

- **MZ** -- Mozambique
- **NA** -- Namibia
- **NC** -- New Caledonia
- **NE** -- Niger
- **NF** -- Norfolk Island
- **NG** -- Nigeria
- **NI** -- Nicaragua
- **NL** -- Netherlands
- **NO** -- Norway
- **NP** -- Nepal
- **NR** -- Nauru
- **NT** -- Neutral Zone
- **NU** -- Niue
- **NZ** -- New Zealand (Aotearoa)
- **OM** -- Oman
- **PA** -- Panama
- **PE** -- Peru
- **PF** -- French Polynesia
- **PG** -- Papua New Guinea
- **PH** -- Philippines
- **PK** -- Pakistan
- **PL** -- Poland
- **PM** -- St. Pierre and Miquelon
- **PN** -- Pitcairn
- **PR** -- Puerto Rico
- **PS** -- Palestinian Territory
- **PT** -- Portugal
- **PW** -- Palau
- **PY** -- Paraguay
- **QA** -- Qatar
- **RE** -- Reunion
- **RO** -- Romania
- **RS** -- Serbia
- **RU** -- Russian Federation
- **RW** -- Rwanda
- **SA** -- Saudi Arabia
- **Sb** -- Solomon Islands
- **SC** -- Seychelles
- **SD** -- Sudan
- **SE** -- Sweden
- **SG** -- Singapore
- **SH** -- St. Helena
- **SI** -- Slovenia
- **SJ** -- Svalbard and Jan Mayen Islands
- **SK** -- Slovak Republic
- **SL** -- Sierra Leone
- **SM** -- San Marino
- **SN** -- Senegal
- **SO** -- Somalia
- **SR** -- Suriname
- **ST** -- Sao Tome and Principe
- **SU** -- USSR (former)

- **SV** -- El Salvador
- **SY** -- Syria
- **SZ** -- Swaziland
- **TC** -- Turks and Caicos Islands
- **TD** -- Chad
- **TF** -- French Southern Territories
- **TG** -- Togo
- **TH** -- Thailand
- **TJ** -- Tajikistan
- **TK** -- Tokelau
- **TM** -- Turkmenistan
- **TN** -- Tunisia
- **TO** -- Tonga
- **TP** -- East Timor
- **TR** -- Turkey
- **TT** -- Trinidad and Tobago
- **TV** -- Tuvalu
- **TW** -- Taiwan
- **TZ** -- Tanzania
- **UA** -- Ukraine
- **UG** -- Uganda
- **UK** -- United Kingdom
- **UM** -- US Minor Outlying Islands
- **US** -- United States
- **UY** -- Uruguay
- **UZ** -- Uzbekistan
- **VA** -- Vatican City State (Holy See)
- **VC** -- Saint Vincent and the Grenadines
- **VE** -- Venezuela
- **VG** -- Virgin Islands (British)
- **VI** -- Virgin Islands (U.S.)
- **VN** -- Viet Nam
- **VU** -- Vanuatu
- **WF** -- Wallis and Futuna Islands
- **WS** -- Samoa
- **YE** -- Yemen
- **YT** -- Mayotte
- **YU** -- Yugoslavia
- **ZA** -- South Africa
- **ZM** -- Zambia
- **ZR** -- Zaire
- **ZW** -- Zimbabwe

end-date

- crypto host-cert generate self-signed *[DATE: START-DATE]* *[DATE: END-DATE]*

  ```
  Validity end date for certificate.
  ```

  Next Available Option:

  - **cname** -- Common name [e.g., IP address of device]. (ASCII-STR) **(p. 137)**

generate

- crypto host-cert generate

  ```
  Create a self-signed certificate for the https server.
  ```

  Next Available Option:
  - **self-signed** -- Create a self-signed certificate for the https server.**(p. 144)**

- crypto key generate

  ```
  Generate a new key.
  ```

  Next Available Options:
  - **cert** -- Install RSA key file for https certificate.**(p. 137)**
  - **ssh** -- Install RSA key file for ssh server.**(p. 144)**
  - **autorun-key** -- Install RSA key file for autorun**(p. 137)**

host-cert

- crypto host-cert

  ```
  Install/remove self-signed certificate for https.
  ```

  Next Available Options:
  - **generate** -- Create a self-signed certificate for the https server.**(p. 143)**
  - **zeroize** -- Delete an existing certificate.**(p. 145)**

key

- crypto key

  ```
  Install/remove RSA key file for ssh or https server.
  ```

  Next Available Options:
  - **generate** -- Generate a new key.**(p. 143)**
  - **zeroize** -- Delete existing key.**(p. 145)**

key-size

- crypto key generate cert rsa *< 512 | 768 | 1024 >*

  Supported Values:
  - **512** -- Install 512-bit RSA key.
  - **768** -- Install 768-bit RSA key.
  - **1024** -- Install 1024-bit RSA key.
- crypto key generate cert *< 512 | 768 | 1024 >*

  Supported Values:
  - **512** -- Install 512-bit RSA key.
  - **768** -- Install 768-bit RSA key.
  - **1024** -- Install 1024-bit RSA key.

organization

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION*

  ```
  Organization name.
  ```

  Next Available Option:
  - **city** -- City or location. (ASCII-STR) **(p. 137)**

org-unit

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT*

  ```
  Organizational unit [Department].
  ```

  Next Available Option:
  - **organization** -- Organization name. (ASCII-STR) **(p. 144)**

rsa

- crypto key generate cert rsa

  ```
  Optional keyword.
  ```

  Next Available Option:
  - **key-size** < 512 | 768 | 1024 > -- **(p. 143)**

- crypto key generate ssh rsa

  ```
  Optional keyword.
  ```

- crypto key generate autorun-key rsa

  ```
  Optional keyword.
  ```

- crypto key zeroize autorun rsa

  ```
  Optional keyword.
  ```

self-signed

- crypto host-cert generate self-signed

  ```
  Create a self-signed certificate for the https server.
  ```

  Next Available Option:
  - **start-date** -- Validity start date for certificate. (MM/DD[/[YY]YY]) **(p. 145)**

ssh

- crypto key generate ssh

  ```
  Install RSA key file for ssh server.
  ```

Next Available Option:

- **rsa** -- Optional keyword.**(p. 144)**

- crypto key zeroize ssh

  ```
  Remove RSA key file for ssh server.
  ```

start-date

- crypto host-cert generate self-signed *[DATE: START-DATE]*

  ```
  Validity start date for certificate.
  ```

  Next Available Option:

  - **end-date** -- Validity end date for certificate. (MM/DD[/[YY]YY]) **(p. 142)**

state

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION CITY STATE*

  ```
  State or region.
  ```

  Next Available Option:

  - **country** < AD | AE | AF | ... > -- Country code (2 character ISO code).**(p. 137)**

zeroize

- crypto host-cert zeroize

  ```
  Delete an existing certificate.
  ```

- crypto key zeroize

  ```
  Delete existing key.
  ```

  Next Available Options:

  - **cert** -- Remove RSA key file for https certificate.**(p. 137)**
  - **ssh** -- Remove RSA key file for ssh server.**(p. 144)**
  - **autorun** -- Remove RSA key file for autorun**(p. 136)**

debug

OVERVIEW

Category:	
Primary context:	manager
Related Commands	**log (page 338)** **show logging (page 486)** **show debug (page 466)**

```
Usage: [no] debug destination <logging|session|buffer>
       [no] debug <all|DEBUG_TYPE>

Description: Enable/disable debug logging.

Parameters:
  o destination - Enable or disable a debug destination. (Multiple
               destinations can be configured)
    o logging - Send the debug messages to a remote device via the syslog
             facility.  System logging must first be enabled with the
             'logging' command.
    o session - Debug messages will be displayed on the current console,
             telnet, or ssh session.
    o buffer - Debug messages will be stored in a limited size in-memory
             buffer, and be available using "show debug buffer".

  o Debug types
    o all - Display messages for all debug types.
    o DEBUG_TYPE - Display debug messages of the specified type.  Use
             <TAB> to see a list of available types and sub-types.
```

COMMAND STRUCTURE

- [no] debug **acl** -- Display debug messages on access control lists. **(p. 147)**
- [no] debug **all** -- Display all debug messages. **(p. 147)**
- [no] debug **arp-protect** -- Display Dynamic ARP Protection messages. **(p. 147)**
- [no] debug **destination < logging | session | buffer >** -- Select destination for debug messages. **(p. 148)**
- [no] debug **dhcp-snooping** -- Display all DHCP Snooping messages. **(p. 148)**
  - **agent** -- Display DHCP Snooping agent messages. **(p. 147)**
  - **event** -- Display DHCP Snooping event messages. **(p. 148)**
  - **packet** -- Display DHCP Snooping packet messages. **(p. 150)**
- [no] debug **event** -- Display event log messages. **(p. 148)**
- [no] debug **ip** -- Display all IP routing messages. **(p. 149)**
  - **ospf** -- Display all OSPF routing messages. **(p. 149)**
    - **adj** -- Display adjacency changes. **(p. 147)**
    - **event** -- Display OSPF events. **(p. 148)**
    - **flood** -- Display information on flood messages. **(p. 148)**
    - **lsa-generation** -- Display new LSAs added to database. **(p. 149)**
    - **packet** -- Display packets sent/received. **(p. 150)**
    - **retransmission** -- Display retransmission timer messages. **(p. 150)**
    - **spf** -- Display path recalculation messages. **(p. 150)**
  - **rip** -- Display all RIP routing messages. **(p. 150)**

        - **database** -- Display database changes. **(p. 147)**
        - **event** -- Display RIP events. **(p. 148)**
        - **trigger** -- Display trigger messages. **(p. 150)**
- [no] debug **ipv6** -- Display debug messages for IPv6. **(p. 149)**
    - **dhcpv6-client** -- Display DHCPv6 client debug messages. **(p. 148)**
        - **events** -- Display DHCPv6 client events. **(p. 148)**
        - **packet** -- Display DHCPv6 client packets. **(p. 150)**
    - **nd** -- Display debug messages for IPv6 neighbor discovery. **(p. 149)**
- [no] debug **lldp** -- Display LLDP information. **(p. 149)**
- [no] debug **wireless-services** -- Display debug messages on wireless-services module. (SLOT-ID-RANGE) **(p. 150)**

COMMAND DETAILS

acl (p. 147)
adj (p. 147)
agent (p. 147)
all (p. 147)
arp-protect (p. 147)
database (p. 147)
destination (p. 148)
dhcp-snooping (p. 148)
dhcpv6-client (p. 148)
event (p. 148)
events (p. 148)
flood (p. 148)
ip (p. 149)
ipv6 (p. 149)
lldp (p. 149)
lsa-generation (p. 149)
nd (p. 149)
ospf (p. 149)
packet (p. 150)
retransmission (p. 150)
rip (p. 150)
spf (p. 150)
trigger (p. 150)
wireless-services (p. 150)

acl

- [no] debug acl

Display debug messages on access control lists.

adj

- [no] debug ip ospf adj

Display adjacency changes.

agent

- [no] debug dhcp-snooping agent

Display DHCP Snooping agent messages.

all

- [no] debug all

Display all debug messages.

arp-protect

- [no] debug arp-protect

Display Dynamic ARP Protection messages.

database

- [no] debug ip rip database

Display database changes.

destination

- [no] debug destination *< logging | session | buffer >*

  ```
  Select destination for debug messages.
  ```

  Supported Values:
  - **logging** -- Send debug messages to syslog server.
  - **session** -- Print debug messages to terminal.
  - **buffer** -- Print debug messages to a buffer in memory.

dhcp-snooping

- [no] debug dhcp-snooping

  ```
  Display all DHCP Snooping messages.
  ```

  Next Available Options:
  - **agent** -- Display DHCP Snooping agent messages.**(p. 147)**
  - **event** -- Display DHCP Snooping event messages.**(p. 148)**
  - **packet** -- Display DHCP Snooping packet messages.**(p. 150)**

dhcpv6-client

- [no] debug ipv6 dhcpv6-client

  ```
  Display DHCPv6 client debug messages.
  ```

  Next Available Options:
  - **events** -- Display DHCPv6 client events.**(p. 148)**
  - **packet** -- Display DHCPv6 client packets.**(p. 150)**

event

- [no] debug dhcp-snooping event

  ```
  Display DHCP Snooping event messages.
  ```

- [no] debug event

  ```
  Display event log messages.
  ```

- [no] debug ip ospf event

  ```
  Display OSPF events.
  ```

- [no] debug ip rip event

  ```
  Display RIP events.
  ```

events

- [no] debug ipv6 dhcpv6-client events

  ```
  Display DHCPv6 client events.
  ```

flood

- [no] debug ip ospf flood

```
Display information on flood messages.
```

ip

- [no] debug ip

```
Display all IP routing messages.
```

Next Available Options:

- **ospf** -- Display all OSPF routing messages.**(p. 149)**
- **rip** -- Display all RIP routing messages.**(p. 150)**

ipv6

- [no] debug ipv6

```
Display debug messages for IPv6.
```

Next Available Options:

- **dhcpv6-client** -- Display DHCPv6 client debug messages.**(p. 148)**
- **nd** -- Display debug messages for IPv6 neighbor discovery.**(p. 149)**

lldp

- [no] debug lldp

```
Display LLDP information.
```

lsa-generation

- [no] debug ip ospf lsa-generation

```
Display new LSAs added to database.
```

nd

- [no] debug ipv6 nd

```
Display debug messages for IPv6 neighbor discovery.
```

ospf

- [no] debug ip ospf

```
Display all OSPF routing messages.
```

Next Available Options:

- **adj** -- Display adjacency changes.**(p. 147)**
- **event** -- Display OSPF events.**(p. 148)**
- **flood** -- Display information on flood messages.**(p. 148)**
- **lsa-generation** -- Display new LSAs added to database.**(p. 149)**
- **packet** -- Display packets sent/received.**(p. 150)**
- **retransmission** -- Display retransmission timer messages.**(p. 150)**
- **spf** -- Display path recalculation messages.**(p. 150)**

packet

- [no] debug dhcp-snooping packet

  ```
  Display DHCP Snooping packet messages.
  ```

- [no] debug ip ospf packet

  ```
  Display packets sent/received.
  ```

- [no] debug ipv6 dhcpv6-client packet

  ```
  Display DHCPv6 client packets.
  ```

retransmission

- [no] debug ip ospf retransmission

  ```
  Display retransmission timer messages.
  ```

rip

- [no] debug ip rip

  ```
  Display all RIP routing messages.
  ```

  Next Available Options:

  - **database** -- Display database changes.**(p. 147)**
  - **event** -- Display RIP events.**(p. 148)**
  - **trigger** -- Display trigger messages.**(p. 150)**

spf

- [no] debug ip ospf spf

  ```
  Display path recalculation messages.
  ```

trigger

- [no] debug ip rip trigger

  ```
  Display trigger messages.
  ```

wireless-services

- [no] debug wireless-services *SLOT-ID-RANGE*

  ```
  Display debug messages on wireless-services module.
  ```

dhcp-relay

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] dhcp-relay
       [no] dhcp-relay [hop-count-increment]
       dhcp-relay [option 82 append[validate]|replace[validate]
                        |drop[validate]|keep [mac|ip]]
       [no] dhcp-relay [option 82 [validate]]

Description: Enable/disable DHCP relay agent on the device.

 hop-count-increment  --- optional argument to 'dhcp-relay' command used to
                  enable/disable increment of hop-count. By default it is
                  enabled.
 option 82    --- optional argument to 'dhcp-relay' command used to specify
                  the operational status (enable/disable) of option 82.
 append|replace|keep|drop ---    argument to 'option 82' command used to
                  specify the policy to apply to client DHCP packets. There
                  is no default option 82 policy defined for the switch.
 validate     --- optional argument to 'option 82' append, replace, and drop
                  sub-arguments used to specify that a validation of the
                  server response packets such that at least one option 82
                  field matches the remote ID of the current switch (multiple
                  option 82 fields may exist, if relay agent is configured
                  using the append policy).
                  If validation fails, the response is considered invalid and
                  thrown away.
 mac          --- Sets the remote ID to be the MAC address of the switch.
                  This is the default value.
 ip           --- Sets the remote ID to be the IP address of the VLAN on
                  which the client request was received.
```

COMMAND STRUCTURE

- [no] dhcp-relay **hop-count-increment** -- Optional argument to dhcp-agent used to enable/disable increment of DHCP hop-count field. **(p. 154)**
- [no] dhcp-relay **option** -- Optional argument to dhcp-agent used to specify operational status for DHCP options. **(p. 156)**
  - **82** -- Optional argument to dhcp-agent used to specify the operational status for option 82. **(p. 153)**
    - **append** -- Specifies that the option 82 field should be appended to client DHCP packet. **(p. 153)**
      - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
      - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
      - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**
      - **validate** -- Specifies the validation for server response. **(p. 157)**
    - **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet. **(p. 153)**

  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**
  - **validate** -- Specifies the validation for server response. **(p. 157)**
- **keep** -- Specifies that no option 82 field will be added or replaced, if option 82 field(s) already exists in the client DHCP packet. **(p. 155)**
  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**
- **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet. **(p. 156)**
  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**
  - **validate** -- Specifies the validation for server response. **(p. 157)**
- **validate** -- Specifies the validation for server response. **(p. 157)**
  - **append** -- Specifies that the option 82 field should be appended to client DHCP packet. **(p. 153)**
    - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
    - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
    - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**
  - **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet. **(p. 153)**
    - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
    - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
    - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**
  - **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet. **(p. 156)**
    - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 154)**
    - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 155)**
    - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 155)**

COMMAND DETAILS

82 (p. 153)
append (p. 153)
drop (p. 153)
hop-count-increment (p. 154)
ip (p. 154)
keep (p. 155)
mac (p. 155)
mgmt-vlan (p. 155)
option (p. 156)
replace (p. 156)
validate (p. 157)

82

- [no] dhcp-relay option 82

```
Optional argument to dhcp-agent used to specify the operational status
for option 82.
```

Next Available Options:

- **append** -- Specifies that the option 82 field should be appended to client DHCP packet.**(p. 153)**
- **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet.**(p. 156)**
- **keep** -- Specifies that no option 82 field will be added or replaced, if option 82 field(s) already exists in the client DHCP packet.**(p. 155)**
- **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet.**(p. 153)**
- **validate** -- Specifies the validation for server response.**(p. 157)**

append

- dhcp-relay option 82 append

```
Specifies that the option 82 field should be appended to client DHCP
packet.
```

Next Available Options:

- **validate** -- Specifies the validation for server response.**(p. 157)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

- dhcp-relay option 82 validate append

```
Specifies that the option 82 field should be appended to client DHCP
packet.
```

Next Available Options:

- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

drop

- dhcp-relay option 82 drop

```
Specifies that the DHCP packet will be dropped unconditionally, if
option 82 field(s) already exists in the client DHCP packet.
```

Next Available Options:

- **validate** -- Specifies the validation for server response.**(p. 157)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**

- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

- dhcp-relay option 82 validate drop

  ```
  Specifies that the DHCP packet will be dropped unconditionally, if
  option 82 field(s) already exists in the client DHCP packet.
  ```

  Next Available Options:

  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

hop-count-increment

- [no] dhcp-relay hop-count-increment

  ```
  Optional argument to dhcp-agent used to enable/disable increment of
  DHCP hop-count field.
  ```

ip

- dhcp-relay option 82 append ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

- dhcp-relay option 82 replace ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

- dhcp-relay option 82 keep ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

- dhcp-relay option 82 drop ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

- dhcp-relay option 82 validate append ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

- dhcp-relay option 82 validate replace ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

- dhcp-relay option 82 validate drop ip

  ```
  Sets the remote id to be the IP address of the VLAN on which the client
  request was received.
  ```

keep

- dhcp-relay option 82 keep

  ```
  Specifies that no option 82 field will be added or replaced, if option 82
  field(s) already exists in the client DHCP packet.
  ```

  Next Available Options:

  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

mac

- dhcp-relay option 82 append mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

- dhcp-relay option 82 replace mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

- dhcp-relay option 82 keep mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

- dhcp-relay option 82 drop mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

- dhcp-relay option 82 validate append mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

- dhcp-relay option 82 validate replace mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

- dhcp-relay option 82 validate drop mac

  ```
  Sets the remote id to be the MAC address of the switch. This is the
  default value.
  ```

mgmt-vlan

- dhcp-relay option 82 append mgmt-vlan

  ```
  Sets the remote id to be the IP address of the Management VLAN.
  ```

- dhcp-relay option 82 replace mgmt-vlan

  ```
  Sets the remote id to be the IP address of the Management VLAN.
  ```

- dhcp-relay option 82 keep mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 drop mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 validate append mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 validate replace mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 validate drop mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

option

- [no] dhcp-relay option

```
Optional argument to dhcp-agent used to specify operational status for
DHCP options.
```

Next Available Option:

- **82** -- Optional argument to dhcp-agent used to specify the operational status for option 82.**(p. 153)**

replace

- dhcp-relay option 82 replace

```
Specifies that any existing option 82 fields will be replaced with
 switch option 82 field for client DHCP packet.
```

Next Available Options:

- **validate** -- Specifies the validation for server response.**(p. 157)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

- dhcp-relay option 82 validate replace

```
Specifies that any existing option 82 fields will be replaced with
 switch option 82 field for client DHCP packet.
```

Next Available Options:

- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 155)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 154)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 155)**

validate

- dhcp-relay option 82 append validate

  ```
  Specifies the validation for server response.
  ```

- dhcp-relay option 82 replace validate

  ```
  Specifies the validation for server response.
  ```

- dhcp-relay option 82 drop validate

  ```
  Specifies the validation for server response.
  ```

- [no] dhcp-relay option 82 validate

  ```
  Specifies the validation for server response.
  ```

Next Available Options:

- **append** -- Specifies that the option 82 field should be appended to client DHCP packet.**(p. 153)**
- **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet.**(p. 156)**
- **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet.**(p. 153)**

dhcp-snooping

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] dhcp-snooping

Description: Enable/Disable the global administrative status of
             DHCP snooping. No snooping will be performed on
             any VLAN if the global administrative status is disabled.
             The default state is disabled.
```

COMMAND STRUCTURE

- [no] dhcp-snooping **authorized-server** -- Configure valid DHCP Servers **(p. 159)**
  - **NONAME1** -- DHCP Server address. (IP-ADDR) **(p. 160)**
- [no] dhcp-snooping **database** -- Configure lease database transfer options **(p. 159)**
  - **delay < 15 to 86400 >** -- Seconds to delay writing to the lease database file. **(p. 160)**
  - **file** -- URL Format: "tftp://<ip-address>/<filename>". (ASCII-STR) **(p. 160)**
  - **timeout < 0 to 86400 >** -- Seconds to wait for the transfer before failing. **(p. 161)**
- [no] dhcp-snooping **option** -- Configure DHCP snooping operational behavior **(p. 160)**
  - **82** -- **(p. 158)**
    - **remote-id < mac | subnet-ip | mgmt-ip >** -- Set relay information option remote-id value to use. (NUMBER) **(p. 161)**
    - **untrusted-policy < drop | keep | replace >** -- Policy for DHCP packets received on untrusted ports thatcontain option 82. (NUMBER) **(p. 161)**
- [no] dhcp-snooping **trust** -- Configure trusted interfaces **(p. 161)**
  - **port-list** -- ([ethernet] PORT-LIST) **(p. 161)**
- [no] dhcp-snooping **verify** -- Enable/Disable DHCP packet validation **(p. 161)**
  - **mac** -- Verify DHCP header client hardware address. **(p. 160)**
- [no] dhcp-snooping **vlan** -- Enable/Disable snooping on a VLAN (VLAN-ID-RANGE) **(p. 162)**
  - **vlan-list** -- (VLAN-ID-RANGE) **(p. 162)**

COMMAND DETAILS

82 (p. 158)
authorized-server (p. 159)
database (p. 159)
delay (p. 160)
file (p. 160)
mac (p. 160)
NONAME1 (p. 160)
option (p. 160)
port-list (p. 161)
remote-id (p. 161)
timeout (p. 161)
trust (p. 161)
untrusted-policy (p. 161)
verify (p. 161)
vlan (p. 162)
vlan-list (p. 162)

82

- [no] dhcp-snooping option 82

Next Available Options:

- **untrusted-policy** < drop | keep | replace > -- Policy for DHCP packets received on untrusted ports thatcontain option 82. (NUMBER) **(p. 161)**

- **remote-id** < mac | subnet-ip | mgmt-ip > -- Set relay information option remote-id value to use. (NUMBER) **(p. 161)**

authorized-server

- [no] dhcp-snooping authorized-server

```
Usage: [no] dhcp-snooping authorized-server <IP-ADDR>

Description: Configure valid DHCP Servers.
             For DHCP Snooping to allow a server to client packet
             to be forwarded, it must be received on a trusted port
             from a valid server. If no authorized servers are configured
             all server addresses are valid. A maximum of 20 authorized
             servers are supported.

Parameters:

    o IP-ADDR - The Address of a trusted DHCP Server.
```

Next Available Option:

- **NONAME1** -- DHCP Server address. (IP-ADDR) **(p. 160)**

database

- [no] dhcp-snooping database

```
Usage: [no] dhcp-snooping database [file ASCII-STR] [delay  <15-86400>]
                                   [timeout <0-86400>]

Description: Configure lease database transfer options.

             No additional parameters are required when 'no' is specified.

Parameters:

    o [file ASCI-STR] - File name in the form of a Universal Resource Locator.
                        The URL must be "tftp://IP-ADDR/ASCII-STR".
                        The max filename length is 63 characters.

    o [delay  <15-86400>]  - Number of seconds to delay writing the database.
                             The default delay is 300 seconds

    o [timeout <0-86400>]  - Number of seconds to wait for the database file
                             transfer to finish before declaring an error.
                             A value of 0 means retry indefinitely.
                             The default timeout is 300 seconds
```

Next Available Options:

- **file** -- URL Format: "tftp://<ip-address>/<filename>". (ASCII-STR) **(p. 160)**
- **delay** < 15 to 86400 > -- Seconds to delay writing to the lease database file.**(p. 160)**
- **timeout** < 0 to 86400 > -- Seconds to wait for the transfer before failing.**(p. 161)**

delay

- dhcp-snooping database delay *< 15 to 86400 >*

```
Seconds to delay writing to the lease database file.
```

Range: < 15 to 86400 >

file

- dhcp-snooping database file *FILE*

```
URL Format: "tftp://<ip-address>/<filename>".
```

mac

- [no] dhcp-snooping verify mac

```
Verify DHCP header client hardware address.
```

NONAME1

- [no] dhcp-snooping authorized-server *IP-ADDR*

```
DHCP Server address.
```

option

- [no] dhcp-snooping option

```
Usage: [no] dhcp-snooping option 82 [remote-id <mac|subnet-ip|mgmt-ip>]
                                    [untrusted-policy <drop|keep|replace>]

Description: Configure DHCP snooping operational behavior.

Parameters:

    o 82 - Add relay information option to DHCP client packets
           that are being forwarded out trusted ports. When 'no'
           is specified, relay information is not inserted.
           The default is to insert relay information.

    o [remote-id <mac|mgmt-ip|subnet-ip>]
         - Set the value used for the remote-id field of the
           relay information option. If 'mac' is specified,
           the switch mac address is used. If 'mgmt-ip' is
           specified, the management vlan ip address is used.
           If 'subnet-ip' is specified, the ip address of the
           VLAN the packet was received on is used. Note that
           when the specified value is 'subnet-ip' or 'mgmt-ip'
           and that value is not set, then the switch mac address
           will be used. The default remote-id is the switch mac.

    o [untrusted-policy <drop|keep|replace>]
         - Configures snooping behavior when forwarding a DHCP
           packet from an untrusted port that has a DHCP relay
           information option present. If 'drop' is specified, the
           packet is dropped. If 'keep' is specified, the packet
           is forwarded without replacing the option. If 'replace'
           is specified the existing option is replaced with one
           generated by this switch. The default is to drop.
```

Next Available Option:

- **82** -- **(p. 158)**

port-list

- [no] dhcp-snooping trust *[ETHERNET] PORT-LIST*

remote-id

- dhcp-snooping option 82 remote-id *< mac | subnet-ip | mgmt-ip >*

```
Set relay information option remote-id value to use.
```

Supported Values:

- **mac** -- switch MAC address.
- **subnet-ip** -- subnet VLAN IP address.
- **mgmt-ip** -- management VLAN IP address.

timeout

- dhcp-snooping database timeout *< 0 to 86400 >*

```
Seconds to wait for the transfer before failing.
```

Range: < 0 to 86400 >

trust

- [no] dhcp-snooping trust

```
Usage: [no] dhcp-snooping trust PORT-LIST

Description: Configure trusted interfaces. Only server packets received
             on trusted interfaces will be forwarded. When 'no' is
             specified the interfaces are marked as untrusted.
             The default port state is untrusted.

Parameters:

    o PORT-LIST - Port list on which to configure trust status.
```

Next Available Option:

- **port-list** -- ([ethernet] PORT-LIST) **(p. 161)**

untrusted-policy

- dhcp-snooping option 82 untrusted-policy *< drop | keep | replace >*

```
Policy for DHCP packets received on untrusted ports thatcontain option 82.
```

Supported Values:

- **drop** -- drop the packet.
- **keep** -- forward the packet unchanged.
- **replace** -- generate new option.

verify

- [no] dhcp-snooping verify

```
Usage: [no] dhcp-snooping verify <mac>

Description: Enable/Disable DHCP packet validation.

Parameters:

    o <mac> - Verify DHCP header client hardware address field
              and the source mac address match for packets received
              on untrusted ports. If 'no' is specified this check is
              omitted. The default is to verify the macs.
```

Next Available Option:

- **mac** -- Verify DHCP header client hardware address.**(p. 160)**

vlan

- dhcp-snooping vlan

```
Usage: [no] dhcp-snooping vlan [VLAN-ID-RANGE ...]
Description: Enable/Disable snooping on a VLAN.
             Note that DHCP snooping must also be globally
             enabled with the 'dhcp-snooping' command for
             snooping to performed on any VLAN. The default state
             is disabled.
Parameters:
    o VLAN-ID-RANGE - VLAN list on which to enable/disable snooping.
```

Next Available Option:

- **vlan-list** -- (VLAN-ID-RANGE) **(p. 162)**

vlan-list

- [no] dhcp-snooping vlan *VLAN-ID-RANGE*

dir

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: dir [<pathname>]

Description: Display a list of the files and subdirectories in a
             directory on a USB device.
```

COMMAND STRUCTURE

- dir **pathname** -- Display a list of the files and subdirectories in a directory on a USB device (ASCII-STR) **(p. 163)**

COMMAND DETAILS

pathname (p. 163)

pathname

- dir *PATHNAME*

```
Usage: dir [<pathname>]

Description: Display a list of the files and subdirectories in a
             directory on a USB device.
```

enable

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	**exit (page 168)** **end (page 165)**

```
Usage: enable

Description: Enter the Manager Exec context.
```

COMMAND STRUCTURE

EXAMPLES

Example: enable

Enter the Manager user name and password to access the Manager Exec context of the CLI:

```
ProCurve> enable
Username: admin1
Password: ########
ProCurve#
```

end

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**exit (page 168)** **enable (page 164)**

```
Usage: end
```

```
Description: Return to the Manager Exec context.
```

COMMAND STRUCTURE

erase

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show config (page 462)** **show port-access (page 495)**

```
Usage: erase <startup-config |
              flash <primary|secondary> |
              config FILENAME>

Description: Erase stored files.

Parameters:
    o startup-config - erase the configuration file loaded
             at the most recent boot.  This will cause an immediate
             reboot with a factory-default configuration.
    o flash <primary|secondary> - erase the specified software image.
    o config FILENAME - erase the specified configuration file.  If
             the config file erased is the one loaded at the most
             recent boot, this will cause an immediate reboot with
             a factory-default configuration.
```

COMMAND STRUCTURE

- erase **config < config | new >** -- Erase the named configuration file **(p. 166)**
- erase **flash < primary | secondary >** -- Erase the primary or secondary flash image **(p. 167)**
- erase **startup-config** -- Erase configuration file. **(p. 167)**

EXAMPLES

Example: erase startup-config

Erase the configuration file used at startup and reset the device to its factory-default configuration:

```
ProCurve(config)# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]?
```

COMMAND DETAILS

config (p. 166)	**flash (p. 167)**	**startup-config (p. 167)**

config

- erase config *< config | new >*

```
Usage: erase config FILENAME

Description: Erase the named configuration file.
```

Supported Values:

- **config**
- **new**

flash

- erase flash *< primary | secondary >*

  ```
  Usage: erase flash <primary|secondary>

  Description: Erase the primary or secondary flash image.
  ```

  Supported Values:
  - **primary** -- Primary flash image.
  - **secondary** -- Secondary flash image.

startup-config

- erase startup-config

  ```
  Erase configuration file.
  ```

exit

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	**end (page 165)** **enable (page 164)**

```
Usage: exit

Description: Return to the previous context or terminate current
             console/telnet session if you are in the Operator context
             level.
```

COMMAND STRUCTURE

EXAMPLES

Example: exit

Exit from the interface configuration context to the global configuration context:

```
ProCurve(eth-A4)# exit
ProCurve(config)#
```

fastboot

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] fastboot
```

```
Description: Enable/disable fastboot on switch.
```

COMMAND STRUCTURE

fault-finder

OVERVIEW

Category:	
Primary context:	config
Related Commands	interface (page 191) show fault-finder (page 471)

```
Usage: [no] fault-finder <all|bad-driver|bad-transceiver|bad-cable|
                          too-long-cable|over-bandwidth|broadcast-storm|
                          loss-of-link>
                         [sensitivity <low|medium|high>]

Description: Enable/disable fault finder and set sensitivity.
             Default is 'sensitivity medium'.
```

COMMAND STRUCTURE

- [no] fault-finder fault-finder **< all | bad-driver | bad-transceiver | ... >** -- Enable/disable fault finder and set sensitivity (p. 170)
- fault-finder sensitivity **< low | medium | high >** -- Define fault finder sensitivity to events. (p. 170)

COMMAND DETAILS

fault-finder (p. 170)	sensitivity (p. 170)

fault-finder

- [no] fault-finder *< all | bad-driver | bad-transceiver | ... >*

```
Usage: [no] fault-finder <all|bad-driver|bad-transceiver|bad-cable|
                          too-long-cable|over-bandwidth|broadcast-storm|
                          loss-of-link>
                         [sensitivity <low|medium|high>]

Description: Enable/disable fault finder and set sensitivity.
             Default is 'sensitivity medium'.
```

Supported Values:

- **all** -- All fault types.
- **bad-driver** -- Too many undersized/giant packets.
- **bad-transceiver** -- Excessive jabbering.
- **bad-cable** -- Excessive CRC/alignment errors.
- **too-long-cable** -- Excessive late collisions.
- **over-bandwidth** -- High collision or drop rate.
- **broadcast-storm** -- Excessive broadcasts.
- **loss-of-link** -- Link lost detected.
- **duplex-mismatch-HDx** -- Duplex Mismatch. Reconfig port to Full Duplex.
- **duplex-mismatch-FDx** -- Duplex Mismatch. Reconfig port to Auto.

sensitivity

- fault-finder sensitivity *< low | medium | high >*

```
Define fault finder sensitivity to events.
```

Supported Values:

- **low** -- Low sensitivity.
- **medium** -- Medium sensitivity.
- **high** -- High sensitivity.

filter

OVERVIEW

Category:	Troubleshooting
Primary context:	config
Related Commands	**connection-rate-filter (page 80)** **ip (page 269)** **show filter (page 472)** **show connection-rate-filter (page 465)**

```
Usage: [no] filter ...

Description: Set or edit traffic/security filters.
             The command allows you to set conditional filters and
             correspondent actions to apply to the incoming traffic
             satisfying to the specified conditions.
             Use 'filter ?' to get a list of all available
             filter types.
```

COMMAND STRUCTURE

- [no] filter **connection-rate** -- Selects behavior for port(s) when a host is filtered **(p. 173)**
  - **connection-rate-portlist** -- ([ethernet] PORT-LIST) **(p. 173)**
    - **filter-action < block | notify-only | throttle >** -- **(p. 174)**
- [no] filter **multicast** -- Specify multicast filter to manage (MAC-ADDR) **(p. 175)**
  - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**
  - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
- [no] filter **protocol < ip | ipx | arp | ... >** -- Specify protocol filter to manage **(p. 176)**
  - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**
  - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
- [no] filter **source-port** -- Specify source-port filter to manage **(p. 176)**
  - **named-filter** -- Set the filter name. **(p. 175)**
    - **ascii** -- Set the filter name. (ASCII-STR) **(p. 173)**
      - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**
      - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
  - **port-list** -- Set the list of source port filters. ([ethernet] PORT-LIST) **(p. 175)**
    - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**
      - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
    - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
      - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**
    - **named-filter** -- Set the filter name. (ASCII-STR) **(p. 175)**

EXAMPLES

Example: filter source-port drop

Create a source-port filter that drops all traffic received on port 5 with a destination of port trunk 1 (trk1) and any port in the range of port 10 to port 15:

```
ProCurve(config)# filter source-port 5 drop trk1,A10-A15
```

Example: filter source-port drop

Create a filter on port trunk 1 to drop traffic received inbound for trunk 2 (trk2) and ports 10-15:

```
ProCurve(config)# filter source-port trk1 drop trk2,A10-A15
```

COMMAND DETAILS

ascii (p. 173)
connection-rate (p. 173)
connection-rate-portlist (p. 173)
drop (p. 174)
filter-action (p. 174)
forward (p. 174)
multicast (p. 175)
named-filter (p. 175)
port-list (p. 175)
protocol (p. 176)
source-port (p. 176)

ascii

- [no] filter source-port named-filter *ASCII*

```
Set the filter name.
```

Next Available Options:

- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**

connection-rate

- [no] filter connection-rate

```
Usage: [no] filter connection-rate port-list  < notify-only | throttle | block>

Description: Selects behavior for port(s) when a host is filtered.
             Block will disable the host until an administrator explicitly
             re-enables access.  Throttle will deny network access for a
             specific penalty period before automatically re-enabling
             access.  Notify will simply log a message/send a SNMP
             trap when the filter is tripped.
```

Next Available Option:

- **connection-rate-portlist** -- ([ethernet] PORT-LIST) **(p. 173)**

connection-rate-portlist

- [no] filter connection-rate *[ETHERNET] PORT-LIST*

Next Available Option:

- **filter-action** < block | notify-only | throttle > -- **(p. 174)**

drop

- filter source-port named-filter *ASCII* drop *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is not permitted.`

- filter source-port *[ETHERNET] PORT-LIST* forward *[ETHERNET] PORT-LIST* drop *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is not permitted.`

- filter source-port *[ETHERNET] PORT-LIST* drop *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is not permitted.`

  Next Available Option:

  - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**

- filter multicast *MAC-ADDR* drop *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is not permitted.`

- filter protocol *< ip | ipx | arp | ... >* drop *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is not permitted.`

filter-action

- filter connection-rate *[ETHERNET] PORT-LIST < block | notify-only | throttle >*

  Supported Values:

  - **block** -- Disable the host until an administrator explicitly re-enables access.
  - **notify-only** -- Log a message/send a SNMP trap when the filter is tripped.
  - **throttle** -- Deny network access for a period before automatically re-enabling access.

forward

- filter source-port named-filter *ASCII* forward *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is permitted.`

- filter source-port *[ETHERNET] PORT-LIST* forward *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is permitted.`

  Next Available Option:

  - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**

- filter source-port *[ETHERNET] PORT-LIST* drop *[ETHERNET] PORT-LIST* forward *[ETHERNET] PORT-LIST*

  `Set a list of ports to which forwarding of filtered packets is permitted.`

- filter multicast *MAC-ADDR* forward *[ETHERNET] PORT-LIST*

```
Set a list of ports to which forwarding of filtered packets is permitted.
```

- filter protocol *< ip | ipx | arp | ... >* forward *[ETHERNET] PORT-LIST*

```
Set a list of ports to which forwarding of filtered packets is permitted.
```

multicast

- [no] filter multicast *MAC-ADDR*

```
Usage: [no] filter multicast MAC-ADDR [...]

Description: Specify multicast filter to manage.
             If preceded by 'no' the command deletes the filter specified.
             Otherwise, the filter is added to the system, if
             it is not already there. Also, an action to apply to the
             packets satisfying to the filter condition can be set.
             The packets satisfying to the filter condition are all
             packets destined to the MAC-ADDR specified. Use
             'filter source-port [ethernet] PORT-NUM ?' to get a list
             of all possible actions that could be applied to the packets.
```

Next Available Options:

- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**

named-filter

- [no] filter source-port named-filter

```
Set the filter name.
```

Next Available Option:

- **ascii** -- Set the filter name. (ASCII-STR) **(p. 173)**

- filter source-port *[ETHERNET] PORT-LIST* named-filter *NAMED-FILTER*

```
Set the filter name.
```

port-list

- [no] filter source-port *[ETHERNET] PORT-LIST*

```
Set the list of source port filters.
```

Next Available Options:

- **named-filter** -- Set the filter name. (ASCII-STR) **(p. 175)**
- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**

protocol

- [no] filter protocol *< ip | ipx | arp | ... >*

```
Usage: [no] filter protocol <ip|ipx|arp|appletalk|sna|netbeui> [...]

Description: Specify protocol filter to manage.
             If preceded by 'no' the command deletes the filter specified.
             Otherwise, the filter is added to the system, if
             it is not already there. Also, an action to apply to the
             packets satisfying to the filter condition can be set.
             The packets satisfying to the filter condition are all
             packets of the protocol specified. Use 'filter source-port
             [ethernet] PORT-NUM ?' to get a list of all possible actions
             that could be applied to the packets.
```

Supported Values:

- **ip**
- **ipx**
- **arp**
- **appletalk**
- **sna**
- **netbeui**

Next Available Options:

- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 174)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 174)**

source-port

- [no] filter source-port

```
Usage: [no] filter source-port [...]

Description: Specify source-port filter to manage.
             Create a named filter,associate source port-list to a
             named-filter and apply actions.The named filter can only be 20
             charactres long.If source port filter is not named,then
             portname is considered as a filter name, and  apply actions to
             received packet on port. If preceded by 'no' the command
             deletes the filter specified.To delete a named-filter use
             no filter source-port named-filter <filter-name> explicitly.
```

Next Available Options:

- **named-filter** -- Set the filter name.**(p. 175)**
- **port-list** -- Set the list of source port filters. ([ethernet] PORT-LIST) **(p. 175)**

front-panel-security

OVERVIEW

Category:	Switch Security
Primary context:	config
Related Commands	

```
Usage: [no] front_panel_security
            <password-clear [reset-on-clear] |
             factory-reset |
             password-recovery>

Description: Enable/disable the ability to clear the password(s) and/or
             configuration via the front panel buttons.  If 'password-clear' is
             disabled, the password(s) cannot be reset using the clear button on
             the front panel of the device.  If 'factory-reset' is disabled, the
             configuration/password(s) can not be reset using the clear and
             reset button combination at boot time.  With 'password-recovery'
             enabled (and the front panel buttons disabled), a lost password can
             be recovered by contacting HP customer support.  With 'password-
             recovery' disabled, there is no way to access a device after losing
             a password with the front panel buttons disabled.
```

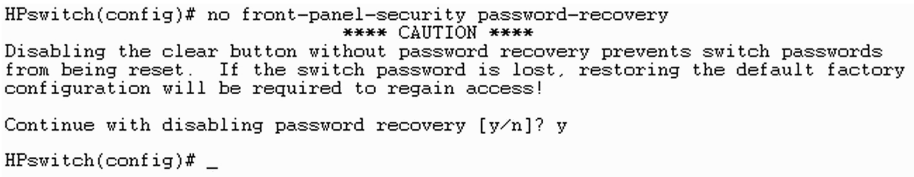
COMMAND STRUCTURE

- [no] front-panel-security **factory-reset** -- Enable/Disable factory-reset ability **(p. 177)**
- [no] front-panel-security **password-clear** -- Enable/Disable password clear **(p. 178)**
  - **reset-on-clear** -- Reset switch on password clear **(p. 178)**
- [no] front-panel-security **password-recovery** -- Enable/Disable password recovery **(p. 178)**

EXAMPLES

Example: no front-panel-security password-recovery

Disable the password-recovery option:



```
HPswitch(config)# no front-panel-security password-recovery
                                   **** CAUTION ****
Disabling the clear button without password recovery prevents switch passwords
from being reset.  If the switch password is lost, restoring the default factory
configuration will be required to regain access!

Continue with disabling password recovery [y/n]? y

HPswitch(config)# _
```

COMMAND DETAILS

factory-reset (p. 177)	**password-recovery (p. 178)**
password-clear (p. 178)	**reset-on-clear (p. 178)**

factory-reset

- [no] front-panel-security factory-reset

```
Enable/Disable factory-reset ability
```

password-clear

- [no] front-panel-security password-clear

```
Enable/Disable password clear
```

Next Available Option:

- **reset-on-clear** -- Reset switch on password clear **(p. 178)**

password-recovery

- [no] front-panel-security password-recovery

```
Usage: [no] front-panel-security password-recovery

Description: Enable/Disable password recovery. To disable 'password-recovery'
             physical access to the front-pannel is required, and within 60 secs
             of pressing the clear button, execute the 'no' form of the command.
```

reset-on-clear

- [no] front-panel-security password-clear reset-on-clear

```
Reset switch on password clear
```

getMIB

OVERVIEW

Category:	manager
Primary context:	manager
Related Commands	**walkMIB (page 655)** **setMIB (page 430)**

```
Usage: getmib OBJECT-STR [OBJECT-STR ...]
```

```
Description: Retrieve and display the value of the MIB objects specified.
```

COMMAND STRUCTURE

- getMIB **object** -- Name and instance of the MIB variable to retrieve. (ASCII-STR) **(p. 179)**

COMMAND DETAILS

object (p. 179)

object

- getMIB *OBJECT*

```
Name and instance of the MIB variable to retrieve.
```

gvrp

OVERVIEW

Category:	config
Primary context:	config
Related Commands	interface (page 191) show gvrp (page 474)

```
Usage: [no] gvrp
```

```
Description: Enable/disable GARP VLAN Registration Protocol (GVRP).
```

COMMAND STRUCTURE

EXAMPLES

Example: gvrp

Enable GVRP on the switch:

```
ProCurve(config)# gvrp
```

hostname

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**snmp-server (page 525)**

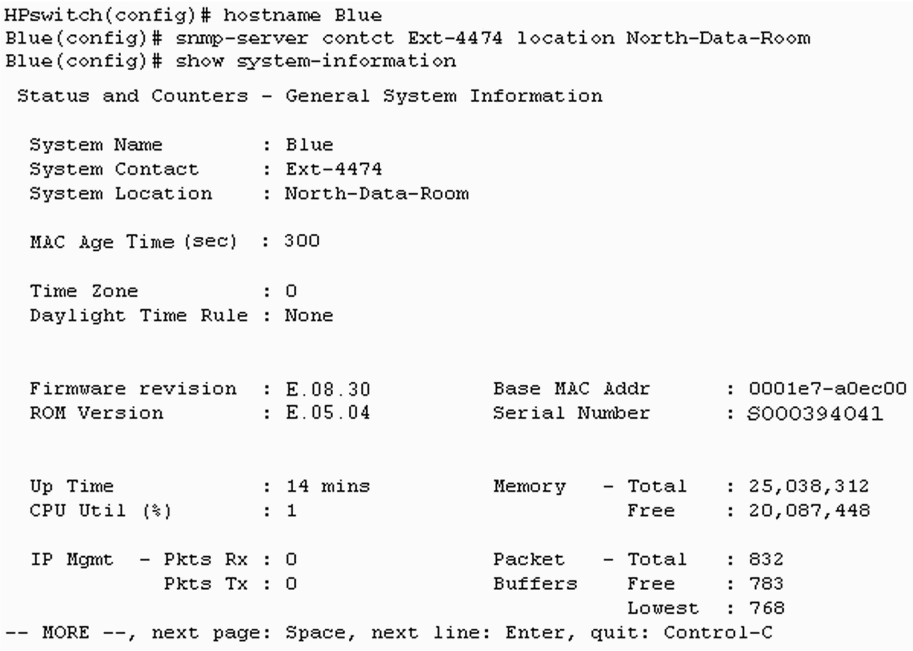
```
Usage: hostname ASCII-STR

Description: Specify the device name for administrative purposes. The
             ASCII-STR defines the device name. It can be up to 30
             characters. Use quotes if your device name contains
             spaces.
```

COMMAND STRUCTURE

EXAMPLES

Example: hostname

Name the switch "Blue" with "Next-4474" as the system contact, and "North-Data-Room" as the location:



```
HPswitch(config)# hostname Blue
Blue(config)# snmp-server contct Ext-4474 location North-Data-Room
Blue(config)# show system-information
 Status and Counters - General System Information

  System Name         : Blue
  System Contact      : Ext-4474
  System Location     : North-Data-Room

  MAC Age Time (sec)  : 300

  Time Zone           : 0
  Daylight Time Rule  : None


  Firmware revision   : E.08.30          Base MAC Addr      : 0001e7-a0ec00
  ROM Version         : E.05.04          Serial Number      : SO00394041


  Up Time             : 14 mins          Memory   - Total   : 25,038,312
  CPU Util (%)        : 1                           Free    : 20,087,448

  IP Mgmt   - Pkts Rx : 0                Packet   - Total   : 832
              Pkts Tx : 0                Buffers    Free    : 783
                                                    Lowest  : 768
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

igmp

OVERVIEW

Category:	IGMP
Primary context:	config
Related Commands	**show igmp (page 476)**

```
Usage: igmp ...

Description: Configure various global IGMP parameters for the switch. The
             'igmp' command must be followed by a feature-specific keyword.
             Use 'igmp ?' to get a list of all possible options.
```

COMMAND STRUCTURE

- igmp **delayed-flush** **< 0 to 255 >** -- Configures the number of seconds an empty IGMP Multicast Group filter will persist in hardware after the last group member leaves **(p. 182)**

COMMAND DETAILS

delayed-flush (p. 182)

delayed-flush

- igmp delayed-flush *< 0 to 255 >*

```
Usage: igmp delayed-flush <0..255>

Description: Configures the number of seconds an empty IGMP Multicast
             Group filter will persist in hardware after the last group
             member leaves. This Delayed Group Flush will drop any further
             'stale' traffic for that group until the timer expires. A
             value of 0 (the default behavior) indicates that the feature
             is disabled.
```

Range: < 0 to 255 >

igmp-proxy-domain

OVERVIEW

Category:	IGMP
Primary context:	config
Related Commands	**show igmp-proxy (page 477)** **vlan (page 611)** **igmp (page 182)**

```
Usage: [no] igmp-proxy-domain DOMAIN-NAME [BORDER-ROUTER-IP-ADDR
       <MCAST-LOW-IP-ADDR MCAST-HIGH-IP-ADDR|all>]

Description: Configure an IGMP proxy domain.
             If the 'no' keyword is used:
                 The DOMAIN-NAME must be specified, All other parameters
                 are optional (they will be verified if they are
                 specified). The specified domain will be deleted if
                 no VLAN associations exist for it.
             If the 'no' keyword is not used:
                 If the DOMAIN-NAME matches the domain name of an
                 existing domain, the respective domain will be updated
                 to reflect the other parameters. Pre-existing proxy
                 entries that are inconsistent after the update will be
                 removed.
                 If the DOMAIN-NAME does not match the domain name of an
                 existing domain, a new domain will be created.
             MCAST-LOW-IP-ADDR and MCAST-HIGH-IP-ADDR
             refer to the low and high inclusive multicast bounds
             respectively. If the keyword 'all' is specified,
             224.0.1.0-239.255.255.255 is used for the inclusive
             multicast bounds.
```

COMMAND STRUCTURE

- [no] igmp-proxy-domain **domain-name** -- Specify the igmp proxy domain name to be added/deleted/updated. (ASCII-STR) **(p. 184)**
  - **border-ip** -- Specify the igmp proxy border ip address. (IP-ADDR) **(p. 184)**
    - **all** -- Specify ALL if the multicast range 224.0.1.0-239.255.255.255 is desired. **(p. 183)**
    - **mcast-low-ip** -- Specify the igmp proxy multicast low bound (inclusive) ip address. (IP-ADDR) **(p. 184)**
      - **mcast-high-ip** -- Specify the igmp proxy multicast high bound (inclusive) ip address. (IP-ADDR) **(p. 184)**

COMMAND DETAILS

all (p. 183)	**domain-name (p. 184)**	**mcast-low-ip (p. 184)**
border-ip (p. 184)	**mcast-high-ip (p. 184)**	

all

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR* all

```
Specify ALL if the multicast range 224.0.1.0-239.255.255.255 is desired.
```

border-ip

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR*

```
Specify the igmp proxy border ip address.
```

Next Available Options:

- **mcast-low-ip** -- Specify the igmp proxy multicast low bound (inclusive) ip address. (IP-ADDR) **(p. 184)**
- **all** -- Specify ALL if the multicast range 224.0.1.0-239.255.255.255 is desired. **(p. 183)**

domain-name

- [no] igmp-proxy-domain *DOMAIN-NAME*

```
Specify the igmp proxy domain name to be added/deleted/updated.
```

Next Available Option:

- **border-ip** -- Specify the igmp proxy border ip address. (IP-ADDR) **(p. 184)**

mcast-high-ip

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR IP-ADDR IP-ADDR*

```
Specify the igmp proxy multicast high bound (inclusive) ip address.
```

mcast-low-ip

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR IP-ADDR*

```
Specify the igmp proxy multicast low bound (inclusive) ip address.
```

Next Available Option:

- **mcast-high-ip** -- Specify the igmp proxy multicast high bound (inclusive) ip address. (IP-ADDR) **(p. 184)**

include-credentials

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] include-credentials

Description: Enable/disable including passwords and credentials in config.
```

NOTES

Benefits

After making changes to security parameters in the running configuration, you can experiment with the new configuration and, if necessary, view the new security settings during the session. After verifying the configuration, you can then save it permanently by writing the settings to the startup-config file.

By permanently saving a switch's security credentials in a configuration file, you can upload the file to a TFTP server or Xmodem host, and later download the file to the ProCurve switches on which you want to use the same security settings without having to manually configure the settings (except for SNMPv3 user parameters) on each switch.

By storing different security settings in different files, you can test different security configurations when you first download a new software version that supports multiple configuration files, by changing the configuration file used when you reboot the switch.

COMMAND STRUCTURE

instrumentation

OVERVIEW

Category:	config
Primary context:	config
Related Commands	

```
Usage: [no] instrumentation monitor [ [<all|arp-requests|ip-address-count|
                                      learn-discards|login-failures|mac-moves|
                                      mac-address-count|pkts-to-closed-ports|
                                      port-auth-failures|system-resource-usage|
                                      system-delay> [<low|med|high|limitValue>]] ]
       [no] instrumentation monitor [trap]
       [no] instrumentation monitor [log]

Description: Enables/Disables instrumentation monitoring.
             The first version of the command enables/disables instrumentation
             monitoring and sets threshold value. By default instrumentation
             monitoring for all parameter is disabled. The command
             'instrumentation monitor all' sets the threshold of each parameter
             to their medium values. The single command 'instrumentation monitor'
             enables/disables instrumentation monitoring for all parameters
             and also enables/disables instrumentation monitoring log.
             The second version of the command enables/disables
             SNMP trap generation. By default SNMP trap generation is disabled.
             Traps are generated if SNMP trap is enabled and counter value
             of the monitoring parameter exceeds the threshold value.
             The third version of the command enables/disables
             instrumentation monitoring log. By default instrumentation
             monitoring log is disabled.

Parameters:

    o all - Enables/Disables instrumentation monitoring for all parameters.
    o arp-requests - Number of ARP requests received.
    o ip-address-count - Number of destination IP addresses learned in the
      IP forwarding table.
    o learn-discards - Number of MAC address learn events per minute
      discarded to help free CPU resources when busy.
    o login-failures - The count of failed CLI login attempts or
      SNMP management authentication failures.
    o mac-moves - The average number of MAC address moves from one port
      to another per minute.
    o mac-address-count - Number of MAC addresses learned in the
      forwarding table.
    o pkts-to-closed-ports - This could indicate a port scan, in which
      an attacker is attempting to expose a vulnerability in the switch.
    o port-auth-failures - The count of times a client has been unsuccessful
      logging into the network.
    o system-resource-usage - Percentage of system resources in use.
    o system-delay - The response time of the CPU to new network events.

    o low - Preconfigured low threshold value.
    o med - Preconfigured medium threshold value.
```

```
o high - Preconfigured high threshold value.
o limitValue - User configured threshold value.
```

COMMAND STRUCTURE

- [no] instrumentation **collection** -- **(p. 187)**
- [no] instrumentation **monitor** -- Enables/Disables instrumentation monitoring **(p. 187)**
  - **log** -- Enables/Disables instrumenation monitoring log. **(p. 187)**
  - **monitor < all | arp-requests | ip-address-count | ... >** -- Enables/Disables instrumentation monitoring **(p. 187)**
    - **limitValue < 1 to 2147483647 >** -- Set the threshold Value. (NUMBER) **(p. 187)**
    - **threshold-value < low | med | high >** -- Set the threshold Value. **(p. 189)**
  - **trap** -- Enables/Disables SNMP trap generation. **(p. 190)**

COMMAND DETAILS

collection (p. 187)	**log (p. 187)**	**threshold-value (p. 189)**
limitValue (p. 187)	**monitor (p. 187)**	**trap (p. 190)**

collection

- [no] instrumentation collection

limitValue

- instrumentation monitor *< all | arp-requests | ip-address-count | ... > < 1 to 2147483647 >*

```
Set the threshold Value.
```

Range: < 1 to 2147483647 >

log

- [no] instrumentation monitor log

```
Enables/Disables instrumenation monitoring log.
```

monitor

- [no] instrumentation monitor

```
Usage: [no] instrumentation monitor [ [<all|arp-requests|ip-address-count|
                                      learn-discards|login-failures|mac-moves|
                                      mac-address-count|pkts-to-closed-ports|
                                      port-auth-failures|system-resource-usage|
                                      system-delay> [<low|med|high|limitValue>]] ]
       [no] instrumentation monitor [trap]
       [no] instrumentation monitor [log]

Description: Enables/Disables instrumentation monitoring.
             The first version of the command enables/disables instrumentation
             monitoring and sets threshold value. By default instrumentation
             monitoring for all parameter is disabled. The command
             'instrumentation monitor all' sets the threshold of each parameter
             to their medium values. The single command 'instrumentation monitor'
             enables/disables instrumentation monitoring for all parameters
             and also enables/disables instrumentation monitoring log.
             The second version of the command enables/disables
             SNMP trap generation. By default SNMP trap generation is disabled.
             Traps are generated if SNMP trap is enabled and counter value
```

```
                of the monitoring parameter exceeds the threshold value.
                The third version of the command enables/disables
                instrumentation monitoring log. By default instrumentation
                monitoring log is disabled.

Parameters:

    o all - Enables/Disables instrumentation monitoring for all parameters.
    o arp-requests - Number of ARP requests received.
    o ip-address-count - Number of destination IP addresses learned in the
      IP forwarding table.
    o learn-discards - Number of MAC address learn events per minute
      discarded to help free CPU resources when busy.
    o login-failures - The count of failed CLI login attempts or
      SNMP management authentication failures.
    o mac-moves - The average number of MAC address moves from one port
      to another per minute.
    o mac-address-count - Number of MAC addresses learned in the
      forwarding table.
    o pkts-to-closed-ports - This could indicate a port scan, in which
      an attacker is attempting to expose a vulnerability in the switch.
    o port-auth-failures - The count of times a client has been unsuccessful
      logging into the network.
    o system-resource-usage - Percentage of system resources in use.
    o system-delay - The response time of the CPU to new network events.

    o low - Preconfigured low threshold value.
    o med - Preconfigured medium threshold value.
    o high - Preconfigured high threshold value.
    o limitValue - User configured threshold value.
```

Next Available Options:

- **monitor** < all | arp-requests | ip-address-count | ... > -- Enables/Disables instrumentation monitoring**(p. 187)**
- **trap** -- Enables/Disables SNMP trap generation. **(p. 190)**
- **log** -- Enables/Disables instrumenation monitoring log. **(p. 187)**

- [no] instrumentation monitor *< all | arp-requests | ip-address-count | ... >*

```
Usage: [no] instrumentation monitor [ [<all|arp-requests|ip-address-count|
                                     learn-discards|login-failures|mac-moves|
                                     mac-address-count|pkts-to-closed-ports|
                                     port-auth-failures|system-resource-usage|
                                     system-delay> [<low|med|high|limitValue>]] ]
       [no] instrumentation monitor [trap]
       [no] instrumentation monitor [log]

Description: Enables/Disables instrumentation monitoring.
             The first version of the command enables/disables instrumentation
             monitoring and sets threshold value. By default instrumentation
             monitoring for all parameter is disabled. The command
             'instrumentation monitor all' sets the threshold of each parameter
             to their medium values. The single command 'instrumentation monitor'
             enables/disables instrumentation monitoring for all parameters
             and also enables/disables instrumentation monitoring log.
             The second version of the command enables/disables
             SNMP trap generation. By default SNMP trap generation is disabled.
             Traps are generated if SNMP trap is enabled and counter value
```

```
                of the monitoring parameter exceeds the threshold value.
                The third version of the command enables/disables
                instrumentation monitoring log. By default instrumentation
                monitoring log is disabled.

Parameters:

    o all - Enables/Disables instrumentation monitoring for all parameters.
    o arp-requests - Number of ARP requests received.
    o ip-address-count - Number of destination IP addresses learned in the
      IP forwarding table.
    o learn-discards - Number of MAC address learn events per minute
      discarded to help free CPU resources when busy.
    o login-failures - The count of failed CLI login attempts or
      SNMP management authentication failures.
    o mac-moves - The average number of MAC address moves from one port
      to another per minute.
    o mac-address-count - Number of MAC addresses learned in the
      forwarding table.
    o pkts-to-closed-ports - This could indicate a port scan, in which
      an attacker is attempting to expose a vulnerability in the switch.
    o port-auth-failures - The count of times a client has been unsuccessful
      logging into the network.
    o system-resource-usage - Percentage of system resources in use.
    o system-delay - The response time of the CPU to new network events.

    o low - Preconfigured low threshold value.
    o med - Preconfigured medium threshold value.
    o high - Preconfigured high threshold value.
    o limitValue - User configured threshold value.
```

Supported Values:

- **all** -- All counter types.
- **arp-requests** -- ARP requests received.
- **ip-address-count** -- IP address count.
- **learn-discards** -- Learn Discards.
- **login-failures** -- Login failures.
- **mac-address-count** -- Mac address count.
- **mac-moves** -- MAC Moves.
- **pkts-to-closed-ports** -- Packets to closed TCP/UDP ports.
- **port-auth-failures** -- Port authentication failures.
- **system-resource-usage** -- System resource usage.
- **system-delay** -- System Delay.

Next Available Options:

- **threshold-value** < low | med | high > -- Set the threshold Value. **(p. 189)**
- **limitValue** < 1 to 2147483647 > -- Set the threshold Value. (NUMBER) **(p. 187)**

threshold-value

- instrumentation monitor *< all | arp-requests | ip-address-count | ... >* *< low | med | high >*

```
Set the threshold Value.
```

Supported Values:

- **low** -- Low threshold.

- **med** -- Medium threshold.
- **high** -- High threshold.

trap

- [no] instrumentation monitor trap

```
Enables/Disables SNMP trap generation.
```

interface

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show interfaces (page 480)**

```
Usage: [no] interface < [ethernet] PORT-LIST [...] | loopback <num> >

Description: Enter the Interface Configuration Level, or execute one
             command for that level. Without optional parameters
             specified, the 'interface' command changes the context to
             the Interface Configuration Context Level for execution of
             configuration changes to the port or ports in the PORT-LIST
             or with loopback keyword it will change context to loopback
             mode. Use 'interface ?' to get a list of all valid commands.
```

COMMAND STRUCTURE

- [no] interface **loopback < 0 to 7 >** -- Enter the loopback Configuration Level **(p. 234)**
  - **ip** -- Configure various IP parameters for the Loopback **(p. 225)**
    - **address** -- Set IP parameters for communication within an IP network **(p. 203)**
      - **ip-addr** -- Interface IP address. (IP-ADDR) **(p. 227)**
    - **ospf** -- configure Open Shortest Path First (OSPF) protocol parameters on the interface **(p. 243)**
      - **all** -- Process the request for all IP addresses. **(p. 207)**
        - **area** -- Specify an OSPF area. **(p. 209)**
          - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
          - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 213)**
        - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 216)**
      - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 227)**
        - **area** -- Specify an OSPF area. **(p. 209)**
          - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
          - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 213)**
        - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 216)**
- [no] interface **port-list** -- Enter the Interface Configuration Level, or execute one command for that level ([ethernet] PORT-LIST) **(p. 248)**
  - **arp-protect** -- Configure the port as trusted or untrusted **(p. 210)**
    - **trust** -- **(p. 264)**
  - **bandwidth-min** -- Enable/disable and configure guaranteed minimum bandwidth settings for outgoing traffic on the port(s) **(p. 214)**
    - **output** -- Enable/disable and configure guaranteed minimum bandwidth for outgoing traffic. **(p. 244)**
      - **queue1 < 0 to 100 >** -- Specify min. bandwidth percentage for queue one outgoing traffic. **(p. 256)**
        - **queue2 < 0 to 100 >** -- Specify min. bandwidth percentage for queue two outgoing traffic. **(p. 256)**
          - **queue3 < 0 to 100 >** -- Specify min. bandwidth percentage for queue three outgoing traffic. **(p. 256)**

          - **queue4 < 0 to 100 >** -- Specify min. bandwidth percentage for queue four outgoing traffic. **(p. 256)**
            - **queue5 < 0 to 100 >** -- Specify min. bandwidth percentage for queue five outgoing traffic. **(p. 257)**
              - *additional options available...*
- **broadcast-limit < 0 to 99 >** -- Set a broadcast traffic percentage limit **(p. 215)**
- **dhcp-snooping** -- Configure the port as trusted or untrusted **(p. 217)**
  - **trust** -- Configure trusted interfaces **(p. 264)**
- **disable** -- Disable port(s) **(p. 218)**
- **enable** -- Enable port(s) **(p. 219)**
- **flow-control** -- Enable/disable flow control on the port(s) **(p. 220)**
- **gvrp** -- Set the GVRP timers on the port (hundredths of a second) **(p. 222)**
  - **join-timer < 20 to 75 >** -- Set join timer value (centiseconds; default 20). **(p. 232)**
  - **leaveall-timer < 500 to 3000 >** -- Set leaveall timer value (centiseconds; default 1000). **(p. 233)**
  - **leave-timer < 40 to 300 >** -- Set leave timer value (centiseconds; default 300). **(p. 233)**
- **ip** -- Apply the specified access control list to inbound packets on this INTERFACE list **(p. 225)**
  - **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list (ASCII-STR) **(p. 201)**
    - **direction < in >** -- **(p. 217)**
- **lacp** -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled **(p. 232)**
  - **mode < Active | Passive >** -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled **(p. 238)**
- **link-keepalive** -- Configure UDLD on port(s) **(p. 233)**
  - **vlan** -- Set vlan-id for tagged UDLD control packets. (VLAN-ID) **(p. 266)**
- **mdix-mode < mdi | mdix | autoMDIX >** -- Set port MDI/MDIX mode (default: auto). **(p. 235)**
- **monitor** -- Define either the port is to be monitored or not **(p. 238)**
  - **all < In | Out | Both >** -- Monitor all traffic. **(p. 207)**
    - **mirror** -- Mirror destination. **(p. 236)**
      - **mirror_session_name** -- Mirror destination name. **(p. 237)**
      - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 241)**
  - **ip** -- Apply an IPv4 access list. **(p. 225)**
    - **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 201)**
      - **monitor_mirror_ACL_dir < In >** -- Define the mirror port for diagnostic purposes **(p. 240)**
        - **mirror** -- Mirror destination. **(p. 236)**
          - **mirror_session_name** -- Mirror destination name. **(p. 237)**
          - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 241)**
- **name** -- Set/unset a name for the port(s) **(p. 242)**
  - **port-name** -- Specify a port name up to 64 characters length. (ASCII-STR) **(p. 249)**
- **poe-allocate-by** -- Control manual power over ethernet allocation **(p. 247)**
  - **allocate_by < usage | class | value >** -- Control manual power over ethernet allocation **(p. 208)**
- **poe-lldp-detect** -- Enabling this feature causes the port to allocate power based on the link-partner's capabilities via LLDP **(p. 247)**
  - **poe_lldp_detect < disabled | enabled >** -- Enabling this feature causes the port to allocate power based on the link-partner's capabilities via LLDP **(p. 246)**
- **poe-value** -- Maximum PoE allocation specified with a value in watts **(p. 248)**
  - **poe_value < 1 | 2 | 3 | ... >** -- Maximum PoE allocation specified with a value in watts **(p. 246)**
- **power-over-ethernet** -- Enable/Disable per-port power distribution **(p. 250)**
  - **priority < critical | high | low >** -- Enable/Disable per-port power distribution **(p. 251)**
- **qinq** -- Configure a port's type as customer-network or provider-network **(p. 254)**

    - **port-type** -- Configure qinq port-type **(p. 249)**
      - **customer-network** -- Configure qinq port-type as customer-network **(p. 216)**
      - **provider-network** -- Configure qinq port-type as provider-network **(p. 254)**
  - **qos** -- Set port-based priority **(p. 254)**
    - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 218)**
    - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 251)**
  - **rate-limit** -- Enable/disable and configure rate-limiting for all traffic (or for incoming ICMP traffic) on the port(s) **(p. 258)**
    - **all** -- Set limits for all traffic. **(p. 207)**
      - **in** -- Set limits for all inbound traffic. **(p. 225)**
        - **kbps < 0 to 10000000 >** -- Specify limit of allowed inbound or outbound traffic in kilobits-per-second on the specified port(s). Actual limits are in steps of 100Kbps to 100Mbps (granularity is 1% of the lowest related media speed). **(p. 232)**
        - **percent < 0 to 100 >** -- Specify limit as percent of inbound or outbound traffic. **(p. 245)**
      - **out** -- Set limits for all outbound traffic. **(p. 244)**
        - **kbps < 0 to 10000000 >** -- Specify limit of allowed inbound or outbound traffic in kilobits-per-second on the specified port(s). Actual limits are in steps of 100Kbps to 100Mbps (granularity is 1% of the lowest related media speed). **(p. 232)**
        - **percent < 0 to 100 >** -- Specify limit as percent of inbound or outbound traffic. **(p. 245)**
    - **icmp** -- Set limits for ICMP traffic only. **(p. 224)**
      - **kbps < 0 to 10000000 >** -- Specify kilobits-per-second limit of allowed ICMP traffic (values should be at least 13Kbps, or max-length ICMP packets will fail.) **(p. 232)**
      - **percent < 0 to 100 >** -- Specify limit as percent of inbound or outbound traffic. **(p. 245)**
    - **ip** -- Apply the specified access control list to inbound packets on this INTERFACE list **(p. 225)**
      - **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list **(p. 201)**
        - **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list (ASCII-STR) **(p. 201)**
          - **direction < in >** -- **(p. 217)**
            - **kbps < 1 to 10000000 >** -- Specify rate-limit in kilo-bits-per-second. (NUMBER) **(p. 232)**
  - **speed-duplex < 10-half | 100-half | 10-full | ... >** -- Define mode of operation for the port(s) **(p. 261)**
  - **type < Trunk | | | ... >** -- **(p. 264)**
  - **unknown-vlans < Learn | Block | Disable >** -- Configure GVRP on the port(s) **(p. 265)**
- [no] interface **svlan** -- Add, delete, edit SVLAN configuration or enter a SVLAN context (VLAN-ID) **(p. 262)**
  - **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 212)**
  - **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter **(p. 215)**
    - **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 265)**
      - **all** -- Resets all previously blocked by the connection rate filter **(p. 207)**
      - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 224)**
      - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 262)**
  - **dhcp-snooping** -- **(p. 217)**
  - **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 220)**
  - **ip** -- Configure various IP parameters for the VLAN **(p. 225)**

    - **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 201)**
      - **direction < in | out | connection-rate-filter | ... >** -- **(p. 217)**
    - **address** -- Set IP parameters for communication within an IP network **(p. 203)**
      - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 217)**
      - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 227)**
  - **ipv6** -- Configure various IP parameters for the VLAN **(p. 230)**
    - **address** -- Set IPv6 parameters for communication within an IP network **(p. 203)**
      - **autoconfig** -- Automatic address configuration. **(p. 213)**
      - **dhcp** -- Configure a DHCPv6 client. **(p. 217)**
        - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server. **(p. 221)**
          - **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server. **(p. 257)**
      - **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 230)**
        - **link-local** -- Configure a link-local IPv6 address. **(p. 234)**
      - **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 231)**
        - **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes **(p. 209)**
        - **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface **(p. 219)**
    - **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr. **(p. 219)**
  - **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size **(p. 232)**
  - **monitor** -- Define either the VLAN is to be monitored or not **(p. 238)**
    - **all < In | Out | Both >** -- Monitor all traffic. **(p. 207)**
      - **mirror** -- Mirror destination. **(p. 236)**
        - **mirror_session_name** -- Mirror destination name. **(p. 237)**
        - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 241)**
    - **ip** -- Apply an IPv4 access list. **(p. 225)**
      - **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 201)**
        - **monitor_mirror_ACL_dir < In >** -- Define the mirror port for diagnostic purposes **(p. 240)**
          - **mirror** -- Mirror destination. **(p. 236)**
            - **mirror_session_name** -- Mirror destination name. **(p. 237)**
            - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 241)**
  - **name** -- Set the VLAN's name (ASCII-STR) **(p. 242)**
  - **protocol** -- Set a predefined protocol for the current VLAN. **(p. 253)**
    - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 253)**
    - **protocols < IPX | IPv4 | IPv6 | ... >** -- Set a predefined protocol for the current VLAN. **(p. 253)**
  - **qos** -- Set VLAN-based priority **(p. 254)**
    - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 218)**
    - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 251)**
  - **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 263)**
  - **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 266)**
  - **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network **(p. 267)**
- [no] interface **vlan** -- Add, delete, edit VLAN configuration or enter a VLAN context (VLAN-ID) **(p. 266)**
  - **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 212)**

- **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter **(p. 215)**
  - **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 265)**
    - **all** -- Resets all previously blocked by the connection rate filter **(p. 207)**
    - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 224)**
    - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 262)**
- **dhcp-snooping** -- **(p. 217)**
- **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 220)**
- **igmp-proxy** -- Associate an IGMP proxy domain with a VLAN **(p. 224)**
  - **domain-name** **< END OF PRINTABLE >** -- Specify the domain name to associate/disassociate with the VLAN. (ASCII-STR) **(p. 218)**
- **ip** -- Configure various IP parameters for the VLAN **(p. 225)**
  - **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 201)**
    - **direction** **< in | out | connection-rate-filter | ... >** -- **(p. 217)**
  - **address** -- Set IP parameters for communication within an IP network **(p. 203)**
    - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 217)**
    - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 227)**
  - **forward-protocol** -- Add or remove a UDP server address for the VLAN **(p. 221)**
    - **udp** -- Add or remove a UDP server address for the VLAN **(p. 265)**
      - **ip-addr** -- IP address of the protocol server. (IP-ADDR) **(p. 227)**
        - **port-name** **< dns | ntp | netbios-ns | ... >** -- (NUMBER) **(p. 249)**
        - **port-num** -- UDP port number of the server. (TCP/UDP-PORT) **(p. 249)**
  - **helper-address** -- Add or remove a DHCP server IP address for the VLAN (IP-ADDR) **(p. 223)**
  - **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature on a VLAN **(p. 224)**
    - **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 212)**
    - **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 214)**
    - **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 219)**
    - **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 220)**
    - **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 221)**
    - **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups **(p. 223)**
    - **querier** -- Specify querier/non-querier capability for the VLAN **(p. 255)**
      - **interval** **< 5 to 300 >** -- Sets the interval in seconds between IGMP queries (default: 125) **(p. 225)**
  - **irdp** -- Configure ICMP Router Discovery Protocol (IRDP) **(p. 231)**
    - **advert-address** **< multicast | broadcast >** -- Specify the destination address to be used for router advertisements **(p. 206)**
    - **holdtime** **< 4 to 9000 >** -- Set the lifetime (in seconds) of the router advertisements sent on this interface **(p. 223)**
    - **maxadvertinterval** **< 4 to 1800 >** -- Set the maximum time (in seconds) allowed between sending unsolicited router advertisements **(p. 235)**
    - **minadvertinterval** **< 3 to 1800 >** -- Set the minimum time (in seconds) allowed between sending unsolicited router advertisements **(p. 236)**
    - **preference** -- The preferability of the router as a default router, relative to the other routers on the same subnet **(p. 250)**

    - **no-default** -- Indicates that the router should never be used as a default by its neighbors. **(p. 243)**
    - **number < -2147483647 to 2147483647 >** -- The router preferability number. Higher values are more preferable. **(p. 243)**
- **local-proxy-arp** -- Enable/disable local proxy ARP **(p. 234)**
- **mroute** -- Configure IP Multicast Routing parameters on the VLAN interface **(p. 242)**
  - **ttl-threshold < 0 to 255 >** -- Set the multicast datagram TTL threshold for the interface **(p. 264)**
- **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the VLAN interface **(p. 243)**
  - **all** -- Process the request for all IP addresses. **(p. 207)**
    - **area** -- Specify an OSPF area. **(p. 209)**
      - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
      - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 213)**
    - **authentication** -- Disable authentication. **(p. 210)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 211)**
      - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 211)**
    - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 216)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 216)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 222)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 235)**
      - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 215)**
    - **passive** -- Configures an ospf interface as passive. **(p. 245)**
    - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 251)**
    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 259)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 263)**
  - **area** -- Specify an OSPF area. **(p. 209)**
    - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
    - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 213)**
  - **authentication** -- Disable authentication. **(p. 210)**
  - **authentication-key** -- Set simple authentication method and key. **(p. 211)**
    - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 211)**
  - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 216)**
  - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 216)**
  - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 222)**
  - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 227)**
    - **area** -- Specify an OSPF area. **(p. 209)**
      - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
      - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 213)**
    - **authentication** -- Disable authentication. **(p. 210)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 211)**
      - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 211)**
    - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 216)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 216)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 222)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 235)**

-
  -
    -
      - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 215)**
    - **passive** -- Configures an ospf interface as passive. **(p. 245)**
    - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 251)**
    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 259)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 263)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 235)**
    - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 215)**
  - **passive** -- Configures an ospf interface as passive. **(p. 245)**
  - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 251)**
  - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 259)**
  - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 263)**
- **pim-dense** -- Enable/disable/configure PIM-DM protocol on the VLAN interface **(p. 245)**
  - **graft-retry-interval < 1 to 10 >** -- Set the interval a PIM router waits for a Graft Ack before resending a Graft on this interface **(p. 222)**
  - **hello-delay < 0 to 5 >** -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface **(p. 222)**
  - **hello-interval < 5 to 300 >** -- Set the frequency at which PIM Hello messages are transmitted on this interface **(p. 222)**
  - **ip-addr** -- Set the source IP address for the PIM-DM packets sent out on this interface **(p. 227)**
    - **any** -- Dynamically determine IP address. **(p. 209)**
    - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 227)**
  - **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface **(p. 233)**
  - **max-graft-retries < 1 to 10 >** -- Set the maximum number of times this router will resend a Graft on this interface **(p. 235)**
  - **override-interval < 500 to 6000 >** -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface **(p. 244)**
  - **propagation-delay < 250 to 2000 >** -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface **(p. 252)**
  - **ttl-threshold < 0 to 255 >** -- Set the Time To Live in a PIM-DM State Refresh message at which it is not forwarded on this interface **(p. 264)**
- **pim-sparse** -- Enable/disable/configure PIM-SM protocol on the VLAN interface **(p. 246)**
  - **dr-priority** -- Set the priority value to use on the interface in the Designated Router election process **(p. 218)**
  - **hello-delay < 0 to 5 >** -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface **(p. 222)**
  - **hello-interval < 5 to 300 >** -- Set the frequency at which PIM Hello messages are transmitted on this interface **(p. 222)**
  - **ip-addr** -- Set the source IP address for the PIM-SM packets sent out on this interface **(p. 227)**
    - **any** -- Dynamically determine IP address. **(p. 209)**
    - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 227)**
  - **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface **(p. 233)**
  - **nbr-timeout < 60 to 8000 >** -- Set the neighbour loss time interval for this interface **(p. 242)**
  - **override-interval < 500 to 6000 >** -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface **(p. 244)**
  - **propagation-delay < 250 to 2000 >** -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface **(p. 252)**
- **proxy-arp** -- Enable/disable proxy ARP **(p. 254)**

  - **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the VLAN interface **(p. 259)**
    - **all** -- Process the request for all IP addresses. **(p. 207)**
      - **authentication-key** -- Set RIP authentication key (maximum 16 characters). **(p. 211)**
        - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 212)**
      - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 212)**
      - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 235)**
      - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 248)**
      - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 258)**
      - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 260)**
      - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 260)**
    - **authentication-key** -- Set RIP authentication key (maximum 16 characters). **(p. 211)**
      - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 212)**
    - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 212)**
    - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 227)**
      - **authentication-key** -- Set RIP authentication key (maximum 16 characters). **(p. 211)**
        - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 212)**
      - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 212)**
      - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 235)**
      - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 248)**
      - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 258)**
      - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 260)**
      - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 260)**
    - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 235)**
    - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 248)**
    - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 258)**
    - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 260)**
    - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 260)**
- **ip-recv-mac-address** -- Associates a L3-mac-address with a VLAN **(p. 229)**
  - **mac-address** -- The L3-mac-address to be associated with a VLAN. (MAC-ADDR) **(p. 234)**
    - **interval** -- Specify the L3-Mac-Address timeout interval. **(p. 225)**
      - **timer-interval < 1 to 255 >** -- Timeout interval in seconds <1-255>. **(p. 263)**
- **ipv6** -- Configure various IP parameters for the VLAN **(p. 230)**
  - **address** -- Set IPv6 parameters for communication within an IP network **(p. 203)**
    - **autoconfig** -- Automatic address configuration. **(p. 213)**
    - **dhcp** -- Configure a DHCPv6 client. **(p. 217)**
      - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server. **(p. 221)**
        - **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server. **(p. 257)**
    - **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 230)**

      - **link-local** -- Configure a link-local IPv6 address. **(p. 234)**
    - **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 231)**
      - **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes **(p. 209)**
      - **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface **(p. 219)**
  - **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr. **(p. 219)**
  - **mld** -- Enable/disable/configure IPv6 Multicast Listener Discovery (MLD) feature on a VLAN **(p. 237)**
    - **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 212)**
    - **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 214)**
    - **fastleave** -- Enables MLD fast-leaves on the specified ports in the selected VLAN ([ethernet] PORT-LIST) **(p. 219)**
    - **forcedfastleave** -- Enables MLD Forced Fast-Leave on the specified ports in the selected VLAN, even if they are cascaded ([ethernet] PORT-LIST) **(p. 220)**
    - **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 221)**
    - **querier** -- This command disables or re-enables the ability for the switch to become querier if necessary **(p. 255)**
- **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size **(p. 232)**
- **monitor** -- Define either the VLAN is to be monitored or not **(p. 238)**
  - **all < In | Out | Both >** -- Monitor all traffic. **(p. 207)**
    - **mirror** -- Mirror destination. **(p. 236)**
      - **mirror_session_name** -- Mirror destination name. **(p. 237)**
      - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 241)**
  - **ip** -- Apply an IPv4 access list. **(p. 225)**
    - **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 201)**
      - **monitor_mirror_ACL_dir < In >** -- Define the mirror port for diagnostic purposes **(p. 240)**
        - **mirror** -- Mirror destination. **(p. 236)**
          - **mirror_session_name** -- Mirror destination name. **(p. 237)**
          - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 241)**
- **name** -- Set the VLAN's name (ASCII-STR) **(p. 242)**
- **protocol** -- Set a predefined protocol for the current VLAN. **(p. 253)**
  - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 253)**
  - **protocols < IPX | IPv4 | IPv6 | ... >** -- Set a predefined protocol for the current VLAN. **(p. 253)**
- **qos** -- Set VLAN-based priority **(p. 254)**
  - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 218)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 251)**
- **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 263)**
- **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 266)**
- **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network **(p. 267)**
- **vrrp** -- Enable/disable/configure VRRP operation on the VLAN **(p. 268)**
  - **vrid < 1 to 255 >** -- Configure a virtual router instance for the VLAN **(p. 268)**
    - **advertise-interval < 1 to 255 >** -- Set time interval (in seconds) between sending VRRP advertisement messages **(p. 206)**

- **backup** -- Designate the virtual router instance as a Backup **(p. 214)**
- **enable** -- Enable/disable operation of the virtual router instance **(p. 219)**
- **owner** -- Designate the virtual router instance as an Owner (Master) **(p. 244)**
- **preempt-delay-time < 1 to 600 >** -- Enable the pre-emptive delay timer for the virtual router instance **(p. 250)**
- **preempt-mode** -- Enable/disable preempt mode for the virtual router instance **(p. 250)**
- **primary-ip-address** -- Specify IP address the virtual router instance will use as a source in VRRP advertisement messages **(p. 251)**
  - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 227)**
  - **lowest** -- Dynamically determine lowest IP address. **(p. 234)**
- **priority < 1 to 255 >** -- Configure priority for the virtual router instance **(p. 251)**
- **virtual-ip-address** -- Specify IP address to be supported by the virtual router instance **(p. 266)**
  - **ip-addr** -- Specify IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 227)**

COMMAND DETAILS

access-group

- [no] interface *[ETHERNET] PORT-LIST* ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

- **direction** < in > -- **(p. 217)**

- interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:

- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 240)**

- [no] interface *[ETHERNET] PORT-LIST* rate-limit ip access-group

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

- **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list (ASCII-STR) **(p. 201)**

- interface *[ETHERNET] PORT-LIST* rate-limit ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

- **direction** < in > -- **(p. 217)**

- [no] interface vlan *VLAN-ID* ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> <in|out>

in                     Match packets this device will route to another VLAN
out                    Match packets this device will route onto this VLAN
vlan                   Match packets that originate within this VLAN
connection-rate-filter Manage new conection rates originating in this VLAN

   Description: Apply the specified access control list on this VLAN interface.
                The ACL can match either packets that are routed from this VLAN
                to another VLAN, packets that will be routed from another VLAN
                to this VLAN, packets that originate on this VLAN, or it can
                manage new connection rates for virus throttling.
```

Next Available Option:

- **direction** < in | out | connection-rate-filter | ... > -- **(p. 217)**

- interface vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:

- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 240)**

- [no] interface svlan *VLAN-ID* ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> <in|out>

in                     Match packets this device will route to another VLAN
out                    Match packets this device will route onto this VLAN
vlan                   Match packets that originate within this VLAN
connection-rate-filter Manage new conection rates originating in this VLAN

   Description: Apply the specified access control list on this VLAN interface.
                The ACL can match either packets that are routed from this VLAN
                to another VLAN, packets that will be routed from another VLAN
                to this VLAN, packets that originate on this VLAN, or it can
                manage new connection rates for virus throttling.
```

Next Available Option:

- **direction** < in | out | connection-rate-filter | ... > -- **(p. 217)**

- interface svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:

- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 240)**

address

- [no] interface loopback *< 0 to 7 >* ip address

```
Usage: [no] ip address [IP-ADDR]

Description: Set IP parameters for communication within an IP network.
             Each loopback Interface represents an IP interface having
              its own unique configuration.  The loopback interface
             for which the configuration is applied can be specified
             implicitly by preceding the phrase 'ip address' with the
```

```
                'interface loopback <num>' keyword and argument.  It
                can also be called explicitly when called directly from a
                Loopback context.  In the latter case the command
                affects the interface identified by the context.

Parameters:

     o IP-ADDR- Assign an IP address to the loopback interface.
       Multiple addresses may be configured on a single loopback interface.
```

Next Available Option:

- **ip-addr** -- Interface IP address. (IP-ADDR) **(p. 227)**

- [no] interface vlan *VLAN-ID* ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.
                Each VLAN represents an IP interface having its own unique
                configuration.  The VLAN for which the configuration is
                applied can be specified implicitly by preceding the
                phrase 'ip address' with the 'vlan VLAN-ID' keyword and
                argument.  It can also be called explicitly when called
                directly from a VLAN context.  In the latter case the
                command affects the VLAN identified by the context.

Parameters:

     o dhcp-bootp - The switch attempts to get its configuration from a
       DHCP/Bootp server.

     o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch or VLAN.
       The IP-ADDR/MASK-LENGTH may be specified in two ways using the
       following syntax:
           ip address 192.32.36.87/24
           ip address 192.32.36.87 255.255.255.0
       Both of the statements above would have the same effect.
       Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 227)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 217)**

- [no] interface vlan *VLAN-ID* ipv6 address

```
Usage: [no] ipv6 address [dhcp|autoconfig|IPv6-ADDR/PREFIX-LEN]

Description: Set IPv6 parameters for communication within an IP network.
                Each VLAN represents an IPv6 interface having its own unique
                configuration.  The VLAN for which the configuration is
                applied can be specified implicitly by preceding the
                phrase 'ipv6 address' with the 'vlan VLAN-ID' keyword and
                argument.  It can also be called explicitly when called
                directly from a VLAN context.  In the latter case the
                command affects the VLAN identified by the context.

Parameters:
    o autoconfig - Enables automatic address configuration of IPv6
      addresses using stateless configuration of an interface .

    o dhcp - The switch attempts to get its configuration from a
      DHCPv6 server.

    o IPv6-ADDR/PREFIX-LEN-Assign an IPv6 address to the switch or VLAN.
      The IPv6-ADDR/PREFIX-LEN may be specified in four ways using the
      following syntax:
          ipv6 address 1234:abcd::5678/40
          ipv6 address 2001:0db8:1:1:ffff:ffff:ffff:fffe/64 anycast
          ipv6 address 2001:0db8:0:1::/64 eui-64
      Only link-local addreses are configured without PREFIX-LEN as below:
          ipv6 address FE80:0:0:0:0123:0456:0789:0abc link-local
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **autoconfig** -- Automatic address configuration.**(p. 213)**
- **dhcp** -- Configure a DHCPv6 client.**(p. 217)**
- **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 230)**
- **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 231)**

- [no] interface svlan *VLAN-ID* ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.
             Each VLAN represents an IP interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ip address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:

    o dhcp-bootp - The switch attempts to get its configuration from a
      DHCP/Bootp server.

    o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch or VLAN.
      The IP-ADDR/MASK-LENGTH may be specified in two ways using the
      following syntax:
          ip address 192.32.36.87/24
          ip address 192.32.36.87 255.255.255.0
      Both of the statements above would have the same effect.
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 227)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 217)**

- [no] interface svlan *VLAN-ID* ipv6 address

```
Usage: [no] ipv6 address [dhcp|autoconfig|IPv6-ADDR/PREFIX-LEN]
```

```
Description: Set IPv6 parameters for communication within an IP network.
             Each VLAN represents an IPv6 interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ipv6 address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:
    o autoconfig - Enables automatic address configuration of IPv6
      addresses using stateless configuration of an interface .

    o dhcp - The switch attempts to get its configuration from a
      DHCPv6 server.

    o IPv6-ADDR/PREFIX-LEN-Assign an IPv6 address to the switch or VLAN.
      The IPv6-ADDR/PREFIX-LEN may be specified in four ways using the
      following syntax:
          ipv6 address 1234:abcd::5678/40
          ipv6 address 2001:0db8:1:1:ffff:ffff:ffff:fffe/64 anycast
          ipv6 address 2001:0db8:0:1::/64 eui-64
      Only link-local addreses are configured without PREFIX-LEN as below:
          ipv6 address FE80:0:0:0:0123:0456:0789:0abc link-local
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **autoconfig** -- Automatic address configuration.**(p. 213)**
- **dhcp** -- Configure a DHCPv6 client.**(p. 217)**
- **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 230)**
- **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 231)**

advert-address

- interface vlan *VLAN-ID* ip irdp *< multicast | broadcast >*

```
Usage: [no] ip irdp <multicast|broadcast>

Description: Specify the destination address to be used for router
             advertisements.
             It has to be either multicast or broadcast. If the value
             of this object is 'multicast' (the default), router
             advertisements will be sent to the all-hosts multicast
             address, 224.0.0.1. If the value of this object is 'broadcast',
             router advertisements sent on this interface will be sent to
             the limitied broadcast address, 255.255.255.255.
```

Supported Values:

- **multicast** -- Send advertisements to all-hosts multicast address.
- **broadcast** -- Send advertisements to broadcast address.

advertise-interval

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* advertise-interval *< 1 to 255 >*

```
Usage: vrrp vrid <VRID> advertise-interval <1-255>
```

```
Description: Set time interval (in seconds) between sending VRRP advertisement
             messages. The default value is one second.
```

Range: < 1 to 255 >

all

- [no] interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >*

  ```
  Monitor all traffic.
  ```

  Supported Values:
  - **In** -- Monitor all inbound traffic
  - **Out** -- Monitor all outbound traffic
  - **Both** -- Monitor all inbound and outbound traffic

  Next Available Option:
  - **mirror** -- Mirror destination.**(p. 236)**

- [no] interface *[ETHERNET] PORT-LIST* rate-limit all

  ```
  Set limits for all traffic.
  ```

  Next Available Options:
  - **in** -- Set limits for all inbound traffic.**(p. 225)**
  - **out** -- Set limits for all outbound traffic.**(p. 244)**

- [no] interface loopback *< 0 to 7 >* ip ospf all

  ```
  Process the request for all IP addresses.
  ```

  Next Available Options:
  - **area** -- Specify an OSPF area.**(p. 209)**
  - **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 216)**

- [no] interface vlan *VLAN-ID* ip ospf all

  ```
  Process the request for all IP addresses.
  ```

  Next Available Options:
  - **passive** -- Configures an ospf interface as passive. **(p. 245)**
  - **area** -- Specify an OSPF area.**(p. 209)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 211)**
  - **authentication** -- Disable authentication.**(p. 210)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 235)**
  - **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 216)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 216)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 222)**
  - **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 251)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 259)**
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 263)**

- [no] interface vlan *VLAN-ID* ip rip all

```
Process the request for all IP addresses.
```

Next Available Options:

- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 212)**
- **authentication-key** -- Set RIP authentication key (maximum 16 characters).**(p. 211)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 235)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 248)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 258)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 260)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 260)**

- interface vlan *VLAN-ID* connection-rate-filter unblock all

```
Resets all previously blocked by the connection rate filter
```

- interface vlan *VLAN-ID* monitor all < *In* | *Out* | *Both* >

```
Monitor all traffic.
```

Supported Values:

- **In** -- Monitor all inbound traffic
- **Out** -- Monitor all outbound traffic
- **Both** -- Monitor all inbound and outbound traffic

Next Available Option:

- **mirror** -- Mirror destination.**(p. 236)**

- interface svlan *VLAN-ID* connection-rate-filter unblock all

```
Resets all previously blocked by the connection rate filter
```

- interface svlan *VLAN-ID* monitor all < *In* | *Out* | *Both* >

```
Monitor all traffic.
```

Supported Values:

- **In** -- Monitor all inbound traffic
- **Out** -- Monitor all outbound traffic
- **Both** -- Monitor all inbound and outbound traffic

Next Available Option:

- **mirror** -- Mirror destination.**(p. 236)**

allocate_by

- interface *[ETHERNET] PORT-LIST* poe-allocate-by < *usage* | *class* | *value* >

```
Usage: poe-allocate-by [usage|class|value]

Description: Control manual power over ethernet allocation.
             By default, power-over-ethernet allocation is automatic by
             usage of the powered device. This can be overriden by manually
```

```
specifying how much power this port should be allocated by
either its class or a user-defined value.
```

Supported Values:

- **usage**
- **class**
- **value**

any

- interface vlan *VLAN-ID* ip pim-dense ip-addr any

  ```
  Dynamically determine IP address.
  ```

- interface vlan *VLAN-ID* ip pim-sparse ip-addr any

  ```
  Dynamically determine IP address.
  ```

anycast

- [no] interface vlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* anycast

  ```
  Address that is assigned to a set of interfaces that typically belong to different
  nodes
  ```

- [no] interface svlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* anycast

  ```
  Address that is assigned to a set of interfaces that typically belong to different
  nodes
  ```

area

- interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* area

  ```
  Specify an OSPF area.
  ```

  Next Available Options:

  - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
  - **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 213)**

- interface loopback *< 0 to 7 >* ip ospf all area

  ```
  Specify an OSPF area.
  ```

  Next Available Options:

  - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
  - **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 213)**

- interface vlan *VLAN-ID* ip ospf area

  ```
  Specify an OSPF area.
  ```

  Next Available Options:

  - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
  - **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 213)**

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* area

```
Specify an OSPF area.
```

Next Available Options:

- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 213)**

- interface vlan *VLAN-ID* ip ospf all area

```
Specify an OSPF area.
```

Next Available Options:

- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 210)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 213)**

area-id

- interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- interface loopback *< 0 to 7 >* ip ospf all area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- interface vlan *VLAN-ID* ip ospf area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- interface vlan *VLAN-ID* ip ospf all area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

arp-protect

- interface *[ETHERNET] PORT-LIST* arp-protect

```
Usage: [no] arp-protect trust

Description: Configure the port as trusted or untrusted. ARP traffic received
             on the untrusted interfaces of ARP Protection enabled VLANs
             are validated against the set of known IP-to-MAC bindings
             maintained by DHCP snooping. By specifying 'no' the port will
             be configured as untrusted. The default state is untrusted.
```

Next Available Option:

- **trust** -- **(p. 264)**

authentication

- [no] interface vlan *VLAN-ID* ip ospf authentication

```
Disable authentication.
```

- [no] interface vlan *VLAN-ID* ip ospf *IP-ADDR* authentication

  ```
  Disable authentication.
  ```

- [no] interface vlan *VLAN-ID* ip ospf all authentication

  ```
  Disable authentication.
  ```

authentication-key

- interface vlan *VLAN-ID* ip ospf authentication-key

  ```
  Set simple authentication method and key.
  ```

  Next Available Option:

  - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 211)**

- interface vlan *VLAN-ID* ip ospf authentication-key *OCTET-STR*

  ```
  OSPF authentication key (maximum 8 characters).
  ```

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* authentication-key

  ```
  Set simple authentication method and key.
  ```

  Next Available Option:

  - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 211)**

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* authentication-key *OCTET-STR*

  ```
  OSPF authentication key (maximum 8 characters).
  ```

- interface vlan *VLAN-ID* ip ospf all authentication-key

  ```
  Set simple authentication method and key.
  ```

  Next Available Option:

  - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 211)**

- interface vlan *VLAN-ID* ip ospf all authentication-key *OCTET-STR*

  ```
  OSPF authentication key (maximum 8 characters).
  ```

- [no] interface vlan *VLAN-ID* ip rip authentication-key

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

  Next Available Option:

  - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 212)**

- [no] interface vlan *VLAN-ID* ip rip *IP-ADDR* authentication-key

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

  Next Available Option:

  - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 212)**

- [no] interface vlan *VLAN-ID* ip rip all authentication-key

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

  Next Available Option:
  - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 212)**

authentication-type

- interface vlan *VLAN-ID* ip rip authentication-type *< none | text >*

  ```
  Set authentication type used on this interface.
  ```

  Supported Values:
  - **none** -- Do not use authentication.
  - **text** -- Use simple password.
- interface vlan *VLAN-ID* ip rip *IP-ADDR* authentication-type *< none | text >*

  ```
  Set authentication type used on this interface.
  ```

  Supported Values:
  - **none** -- Do not use authentication.
  - **text** -- Use simple password.
- interface vlan *VLAN-ID* ip rip all authentication-type *< none | text >*

  ```
  Set authentication type used on this interface.
  ```

  Supported Values:
  - **none** -- Do not use authentication.
  - **text** -- Use simple password.

auth-key-text

- interface vlan *VLAN-ID* ip rip authentication-key *OCTET-STR*

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

- interface vlan *VLAN-ID* ip rip *IP-ADDR* authentication-key *OCTET-STR*

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

- interface vlan *VLAN-ID* ip rip all authentication-key *OCTET-STR*

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

auto

- interface vlan *VLAN-ID* auto *[ETHERNET] PORT-LIST*

  ```
  Usage: [no] auto [ethernet] PORT-LIST

  Description: Cause each port identified in the port list to learn its
               VLAN membership using the GARP VLAN Registration Protocol
               (GVRP). This command is only valid when GVRP is enabled.
               This is a VLAN context command. It can be called directly
               from the VLAN context or follow the 'vlan VLAN-ID'
               command.
  ```

- interface vlan *VLAN-ID* ip igmp auto *[ETHERNET] PORT-LIST*

```
Usage: ip igmp auto [ethernet] PORT-LIST

Description: Instruct the device to monitor incoming multicast traffic
             on the specified ports (this is the default behavior).  This
             feature is configured on a per-VLAN basis.
```

- interface vlan *VLAN-ID* ipv6 mld auto *[ETHERNET] PORT-LIST*

```
Usage: vlan < vid > ipv6 mld auto < port-list >

Description: Instruct the device to monitor incoming multicast traffic
             on the specified ports (this is the default behavior).  This
             feature is configured on a per-VLAN basis.
```

- interface svlan *VLAN-ID* auto *[ETHERNET] PORT-LIST*

```
Usage: [no] auto [ethernet] PORT-LIST

Description: Cause each port identified in the port list to learn its
             VLAN membership using the GARP VLAN Registration Protocol
             (GVRP). This command is only valid when GVRP is enabled.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

autoconfig

- [no] interface vlan *VLAN-ID* ipv6 address autoconfig

```
Automatic address configuration.
```

- [no] interface svlan *VLAN-ID* ipv6 address autoconfig

```
Automatic address configuration.
```

backbone

- interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* area backbone

```
The backbone area (the same as 0.0.0.0).
```

- interface loopback *< 0 to 7 >* ip ospf all area backbone

```
The backbone area (the same as 0.0.0.0).
```

- interface vlan *VLAN-ID* ip ospf area backbone

```
The backbone area (the same as 0.0.0.0).
```

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* area backbone

```
The backbone area (the same as 0.0.0.0).
```

- interface vlan *VLAN-ID* ip ospf all area backbone

```
The backbone area (the same as 0.0.0.0).
```

backup

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* backup

```
Usage: vrrp vrid <VRID> backup

Description: Designate the virtual router instance as a Backup.
             There is no default value.
```

bandwidth-min

- interface *[ETHERNET] PORT-LIST* bandwidth-min

```
Usage: bandwidth-min output <0-100> <0-100> <0-100> <0-100>
                            <0-100> <0-100> <0-100> <0-100>
       no bandwidth-min output

Description: Enable/disable and configure guaranteed minimum bandwidth
             settings for outgoing traffic on the port(s). By default,
             guaranteed minimum bandwidth is configured with a recommended
             profile for outgoing traffic that prevents higher-priority
             queues from starving lower-priority traffic.
             When the feature is enabled, the value for each of the
             queues indicates the minimum percentage of port throughput that
             will be guaranteed for that queue. If a given queue does not
             require its guaranteed minimum in a given service window, any
             extra bandwidth is allocated to the other queues, beginning
             with the highest-priority queue.
             The actual number of queues could be 2, 4 or 8, depending on
             system default and command 'qos queue-config N-queues'.
             The sum of all configured queue values must not exceed 100%.
             Per-queue values must be specified starting with queue one
             being the lowest priority and queue eight being the highest
             priority.
             If no guaranteed minimum bandwidth is configured (i.e., the
             settings for all queues are 0), the traffic is serviced
             strictly by priority. In practice, this may cause complete
             starvation of some or all lower-priority queues during any
             periods where the output port traffic is over-subscribed.
             This is an Interface context command. It can be called directly
             from the interface context, or following the
             'interface [ethernet] PORT-LIST' command.
```

Next Available Option:

- **output** -- Enable/disable and configure guaranteed minimum bandwidth for outgoing traffic.**(p. 244)**

blocked

- interface vlan *VLAN-ID* ip igmp blocked *[ETHERNET] PORT-LIST*

```
Usage: ip igmp blocked [ethernet] PORT-LIST

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

- interface vlan *VLAN-ID* ipv6 mld blocked *[ETHERNET] PORT-LIST*

```
Usage: vlan < vid > ipv6 mld blocked < port-list >

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

broadcast-limit

- interface *[ETHERNET] PORT-LIST* broadcast-limit *< 0 to 99 >*

```
Usage: broadcast-limit <0-99>

Description: Set a broadcast traffic percentage limit.
             This command sets the theoretical maximum of network
             bandwidth in percentage that can be used for broadcast
             traffic. Any broadcast traffic exceeding that limit will be
             dropped. '0' means the feature is disabled.
             For 1000 Mbps and higher speed ports, the percentage of broadcast
             traffic configured is that percentage applied to the theoretical
             maximum broadcast throughput for a 100 Mbps port.  This is to
             allow finer resolution of control for high-speed links.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Range: < 0 to 99 >

chain-name

- interface vlan *VLAN-ID* ip ospf md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- interface vlan *VLAN-ID* ip ospf all md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

connection-rate-filter

- interface vlan *VLAN-ID* connection-rate-filter

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK
>
       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Re-enables access to a host or set of hosts  that has been previously
             blocked by the connection rate filter. Disabling or setting sensitivity

             may have improved performance after rebooting the switch
```

Next Available Option:

- **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 265)**

- interface svlan *VLAN-ID* connection-rate-filter

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK >

       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Re-enables access to a host or set of hosts  that has been previously
             blocked by the connection rate filter. Disabling or setting sensitivity

             may have improved performance after rebooting the switch
```

Next Available Option:

- **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 265)**

cost

- interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* cost *< 1 to 65535 >*

  ```
  Set metric of this interface.
  ```

  Range: < 1 to 65535 >
- interface loopback *< 0 to 7 >* ip ospf all cost *< 1 to 65535 >*

  ```
  Set metric of this interface.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip ospf cost *< 1 to 65535 >*

  ```
  Set metric of this interface.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip ospf *IP-ADDR* cost *< 1 to 65535 >*

  ```
  Set metric of this interface.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip ospf all cost *< 1 to 65535 >*

  ```
  Set metric of this interface.
  ```

  Range: < 1 to 65535 >

customer-network

- interface *[ETHERNET] PORT-LIST* qinq port-type customer-network

  ```
  Configure qinq port-type as customer-network
  ```

dead-interval

- interface vlan *VLAN-ID* ip ospf dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip ospf *IP-ADDR* dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip ospf all dead-interval *< 1 to 65535 >*

```
Set dead interval in seconds; the default is 40.
```

Range: < 1 to 65535 >

dhcp

- [no] interface vlan *VLAN-ID* ipv6 address dhcp

  ```
  Configure a DHCPv6 client.
  ```

  Next Available Option:
  - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server.**(p. 221)**

- [no] interface svlan *VLAN-ID* ipv6 address dhcp

  ```
  Configure a DHCPv6 client.
  ```

  Next Available Option:
  - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server.**(p. 221)**

dhcp-bootp

- interface vlan *VLAN-ID* ip address dhcp-bootp

  ```
  Configure the interface to use DHCP/Bootp server to acquire parameters.
  ```

- interface svlan *VLAN-ID* ip address dhcp-bootp

  ```
  Configure the interface to use DHCP/Bootp server to acquire parameters.
  ```

dhcp-snooping

- interface *[ETHERNET] PORT-LIST* dhcp-snooping

  ```
  Usage: [no] dhcp-snooping trust

  Description: Configure the port as trusted or untrusted. Only DHCP server
               packets received on trusted interfaces will be forwarded.
               By specifying 'no' the port will be configured as untrusted.
               The default state is untrusted.
  ```

  Next Available Option:
  - **trust** -- Configure trusted interfaces**(p. 264)**

- [no] interface vlan *VLAN-ID* dhcp-snooping

- [no] interface svlan *VLAN-ID* dhcp-snooping

direction

- [no] interface *[ETHERNET] PORT-LIST* ip access-group *ACCESS-GROUP* *< in >*

  Supported Values:
  - **in** -- Match inbound packets
- interface *[ETHERNET] PORT-LIST* rate-limit ip access-group *ACCESS-GROUP* *< in >*

  Supported Values:

- **in** -- Configure for inbound traffic

Next Available Option:

- **kbps** < 1 to 10000000 > -- Specify rate-limit in kilo-bits-per-second. (NUMBER) **(p. 232)**

- [no] interface vlan *VLAN-ID* ip access-group *ACCESS-GROUP < in | out | connection-rate-filter | ... >*

  Supported Values:
  - **in** -- Match inbound packets
  - **out** -- Match outbound packets
  - **connection-rate-filter** -- Manage packet rates
  - **vlan** -- VLAN acl
- [no] interface svlan *VLAN-ID* ip access-group *ACCESS-GROUP < in | out | connection-rate-filter | ... >*

  Supported Values:
  - **in** -- Match inbound packets
  - **out** -- Match outbound packets
  - **connection-rate-filter** -- Manage packet rates
  - **vlan** -- VLAN acl

disable

- interface *[ETHERNET] PORT-LIST* disable

```
Usage: disable

Description: Disable port(s).
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

domain-name

- [no] interface vlan *VLAN-ID* igmp-proxy *< END OF PRINTABLE >*

```
Specify the domain name to associate/disassociate with the VLAN.
```

  Supported Values:
  - **END OF PRINTABLE**

dr-priority

- interface vlan *VLAN-ID* ip pim-sparse dr-priority *INTEGER*

```
Usage: ip pim-sparse dr-priority <0-2147483647>

Description: Set the priority value to use on the interface in the Designated
             Router election process. Default is 1.
```

dscp

- interface *[ETHERNET] PORT-LIST* qos dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

  Supported Values:

Binary formatted value from 000000 to 111111

- interface vlan *VLAN-ID* qos dscp *< 000000 | 000001 | 000010 | ... >*

  ```
  Specify DSCP policy to use.
  ```

  Supported Values:

  Binary formatted value from 000000 to 111111

- interface svlan *VLAN-ID* qos dscp *< 000000 | 000001 | 000010 | ... >*

  ```
  Specify DSCP policy to use.
  ```

  Supported Values:

  Binary formatted value from 000000 to 111111

enable

- interface *[ETHERNET] PORT-LIST* enable

  ```
  Usage: enable

  Description: Enable port(s).
               This is an Interface context command. It can be called directly
               from the interface context or follow the 'interface [ethernet]
               PORT-LIST' command.
  ```

- [no] interface vlan *VLAN-ID* ipv6 enable

  ```
  Enable IPv6 on an interface and configures an automatically generated link-local addr.
  ```

- [no] interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* enable

  ```
  Usage: [no] vrrp vrid <VRID> enable

  Description: Enable/disable operation of the virtual router instance.
               The default value is 'disabled'.
  ```

- [no] interface svlan *VLAN-ID* ipv6 enable

  ```
  Enable IPv6 on an interface and configures an automatically generated link-local addr.
  ```

eui-64

- [no] interface vlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* eui-64

  ```
  An IPv6 EUI-64 address that can be automatically configured on any interface
  ```

- [no] interface svlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* eui-64

  ```
  An IPv6 EUI-64 address that can be automatically configured on any interface
  ```

fastleave

- [no] interface vlan *VLAN-ID* ip igmp fastleave *[ETHERNET] PORT-LIST*

  ```
  Usage: [no] ip igmp fastleave [ethernet] PORT-LIST

  Description: Enables or disables IGMP Fast Leaves. When enabled, as soon as
               an IGMP Group Leave has been received on a non-cascaded port,
               the switch stops forwarding multicast traffic for that group
  ```

```
               to that port.
               Does not apply to cascaded ports (see ip igmp forcedfastleave).
               When disabled, or when the port is cascaded, the regular IGMP
               leave time is used (up to 10 seconds when the switch is not
               the IGMP Querier).
               The default behavior is for IGMP FastLeaves to be enabled.
               This feature is configured for ports on a per-VLAN basis.
```

- [no] interface vlan *VLAN-ID* ipv6 mld fastleave *[ETHERNET] PORT-LIST*

```
Usage:  [no] ipv6 mld fastleave < port-list >

Description: Enables MLD fast-leaves on the specified ports in the selected VLAN.
             The no form of the command disables MLD fast-leave on the specified
             ports in the selected VLAN.
```

flow-control

- [no] interface *[ETHERNET] PORT-LIST* flow-control

```
Usage: [no] flow-control

Description: Enable/disable flow control on the port(s). By default,
             flow control is disabled. Flow Control is enabled on both
             transmit and receive or auto negotiated if port Mode is set
             to Auto.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

forbid

- [no] interface vlan *VLAN-ID* forbid *[ETHERNET] PORT-LIST*

```
Usage: [no] forbid [ethernet] PORT-LIST

Description: Prevent ports from becoming a member of the current VLAN.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- [no] interface svlan *VLAN-ID* forbid *[ETHERNET] PORT-LIST*

```
Usage: [no] forbid [ethernet] PORT-LIST

Description: Prevent ports from becoming a member of the current VLAN.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

forcedfastleave

- [no] interface vlan *VLAN-ID* ip igmp forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forcedfastleave [ethernet] PORT-LIST

Description: When enabled, this feature forces IGMP Fast Leaves to occur
             even when the port is cascaded. See 'ip igmp fastleave' for
             more information.  The default behavior is for IGMP Forced
```

```
                FastLeaves to be disabled.
                This feature is configured for ports on a per-VLAN basis.
```

- [no] interface vlan *VLAN-ID* ipv6 mld forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] vlan < vid > ipv6 mld forcedfastleave <port-list>

Description: Enables MLD Forced Fast-Leave on the specified ports in the selected
VLAN,
                even if they are cascaded. (Default: Disabled.)  The no form of the
command
                disables Forced Fast-Leave on the specified ports in the selected VLAN
```

forward

- interface vlan *VLAN-ID* ip igmp forward *[ETHERNET] PORT-LIST*

```
Usage: ip igmp forward [ethernet] PORT-LIST

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

- interface vlan *VLAN-ID* ipv6 mld forward *[ETHERNET] PORT-LIST*

```
Usage: vlan < vid > ipv6 mld forward < port-list >

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

forward-protocol

- interface vlan *VLAN-ID* ip forward-protocol

```
Usage: [no] ip forward-protocol udp IP-ADDR PORT-NUM|PORT-NAME

Description: Add or remove a UDP server address for the VLAN. The
             broadcast  packets received by the switch on this VLAN are to
             be forwarded to the specified application server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **udp** -- Add or remove a UDP server address for the VLAN**(p. 265)**

full

- [no] interface vlan *VLAN-ID* ipv6 address dhcp full

```
Obtain IPv6 address & Configuration information from DHCPv6 server.
```

Next Available Option:

- **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server.**(p. 257)**

- [no] interface svlan *VLAN-ID* ipv6 address dhcp full

```
Obtain IPv6 address & Configuration information from DHCPv6 server.
```

Next Available Option:

- **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server.**(p. 257)**

graft-retry-interval

- interface vlan *VLAN-ID* ip pim-dense graft-retry-interval *< 1 to 10 >*

```
Usage: ip pim-dense graft-retry-interval <1-10>

Description: Set the interval a PIM router waits for a Graft Ack before
             resending a Graft on this interface. Default value is 3
             seconds.
```

Range: < 1 to 10 >

gvrp

- interface *[ETHERNET] PORT-LIST* gvrp

```
Usage: gvrp [join-timer <n>][leave-timer <n>][leaveall-timer <n>]

Description: Set the GVRP timers on the port (hundredths of a second).
             The timers must follow the constraints
             2 * join-timer  <=  leave-timer  <  leaveall-timer
```

Next Available Options:

- **join-timer** < 20 to 75 > -- Set join timer value (centiseconds; default 20).**(p. 232)**
- **leave-timer** < 40 to 300 > -- Set leave timer value (centiseconds; default 300).**(p. 233)**
- **leaveall-timer** < 500 to 3000 > -- Set leaveall timer value (centiseconds; default 1000).**(p. 233)**

hello-delay

- interface vlan *VLAN-ID* ip pim-dense hello-delay *< 0 to 5 >*

```
Usage: ip pim-dense hello-delay <0-5>

Description: Set the maximum time before a triggered PIM Hello message is
             transmitted on this interface. Default value is 5 seconds.
```

Range: < 0 to 5 >

- interface vlan *VLAN-ID* ip pim-sparse hello-delay *< 0 to 5 >*

```
Usage: ip pim-sparse hello-delay <0-5>

Description: Set the maximum time before a triggered PIM Hello message is
             transmitted on this interface. Default value is 5 seconds.
```

Range: < 0 to 5 >

hello-interval

- interface vlan *VLAN-ID* ip ospf hello-interval *< 1 to 65535 >*

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* hello-interval *< 1 to 65535 >*

  ```
  Set hello interval in seconds; the default is 10.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip ospf all hello-interval *< 1 to 65535 >*

  ```
  Set hello interval in seconds; the default is 10.
  ```

  Range: < 1 to 65535 >
- interface vlan *VLAN-ID* ip pim-dense hello-interval *< 5 to 300 >*

  ```
  Usage: ip pim-dense hello-interval <5-300>

  Description: Set the frequency at which PIM Hello messages are transmitted
               on this interface. Default value is 30 seconds.
  ```

  Range: < 5 to 300 >
- interface vlan *VLAN-ID* ip pim-sparse hello-interval *< 5 to 300 >*

  ```
  Usage: ip pim-sparse hello-interval <5-300>

  Description: Set the frequency at which PIM Hello messages are transmitted
               on this interface. Default value is 30 seconds.
  ```

  Range: < 5 to 300 >

helper-address

- [no] interface vlan *VLAN-ID* ip helper-address *IP-ADDR*

  ```
  Usage: [no] ip helper-address IP-ADDR

  Description: Add or remove a DHCP server IP address for the VLAN. The
               DHCP requests received by the switch on this VLAN are to
               be relayed to the specified DHCP server.
               This is a VLAN context command. It can be called directly
               from the VLAN context or follow the 'vlan VLAN-ID'
               command.
  ```

high-priority-forward

- [no] interface vlan *VLAN-ID* ip igmp high-priority-forward

  ```
  Usage: [no] ip igmp high-priority-forward

  Description: Enable/disable the high priority forwarding of traffic for
               subscribed IP Multicast groups. This feature is configured on
               a per-VLAN  basis.
  ```

holdtime

- interface vlan *VLAN-ID* ip irdp holdtime *< 4 to 9000 >*

  ```
  Usage: [no] ip irdp holdtime <4-9000>

  Description: Set the lifetime (in seconds) of the router advertisements sent
               on this interface. Must be no less than the maximum time
               allowed between sending unsolicited router advertisements.
  ```

  Range: < 4 to 9000 >

host

- interface vlan *VLAN-ID* connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

- interface svlan *VLAN-ID* connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

icmp

- [no] interface *[ETHERNET] PORT-LIST* rate-limit icmp

```
Set limits for ICMP traffic only.
```

Next Available Options:

- **percent** < 0 to 100 > -- Specify limit as percent of inbound or outbound traffic.**(p. 245)**
- **kbps** < 0 to 10000000 > -- Specify kilobits-per-second limit of allowed ICMP traffic (values should be at least 13Kbps, or max-length ICMP packets will fail.) **(p. 232)**

igmp

- [no] interface vlan *VLAN-ID* ip igmp

```
Usage: [no] ip igmp [...]

Description: Enable/disable/configure IP Multicast Group Protocol (IGMP)
             feature on a VLAN.  This command enables, disables or
             configures the IGMP feature for IGMP communication between
             Multicast Routers, Multicast Servers, and Multicast Clients
             connected to the device.  This is a VLAN context command. It
             can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix.  If not preceded by 'no',
             the command accepts a variety of configuration parameters. To
             get a list of all available parameters use 'ip igmp ?'. To
             get detailed help for a parameter follow it with 'help'
             keyword.
```

Next Available Options:

- **querier** -- Specify querier/non-querier capability for the VLAN**(p. 255)**
- **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups**(p. 223)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 212)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 214)**
- **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 219)**
- **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 220)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 221)**

igmp-proxy

- [no] interface vlan *VLAN-ID* igmp-proxy

```
Usage: [no] igmp-proxy DOMAIN-NAME

Description: Associate an IGMP proxy domain with a VLAN.
             If the 'no' keyword is used:
                 If the DOMAIN-NAME is left blank, all the domains
                 associated with the respective VLAN will be disassociated.
                 If a DOMAIN-NAME is specified, The specified domain will
                 be disassociated from the respecive VLAN.
             If the 'no' keyword is not used:
                 If the DOMAIN-NAME matches the domain name of an
                 existing domain, the respective domain will be associated
                 with the respective VLAN.
```

Next Available Option:

- **domain-name** < END OF PRINTABLE > -- Specify the domain name to associate/disassociate with the VLAN. (ASCII-STR) **(p. 218)**

in

- [no] interface *[ETHERNET] PORT-LIST* rate-limit all in

```
Set limits for all inbound traffic.
```

Next Available Options:

- **percent** < 0 to 100 > -- Specify limit as percent of inbound or outbound traffic.**(p. 245)**
- **kbps** < 0 to 10000000 > -- Specify limit of allowed inbound or outbound traffic in kilobits-per-second on the specified port(s). Actual limits are in steps of 100Kbps to 100Mbps (granularity is 1% of the lowest related media speed). **(p. 232)**

interval

- interface vlan *VLAN-ID* ip igmp querier interval *< 5 to 300 >*

```
Sets the interval in seconds between IGMP queries
 (default: 125)
```

Range: < 5 to 300 >

- interface vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR* interval

```
Specify the L3-Mac-Address timeout interval.
```

Next Available Option:

- **timer-interval** < 1 to 255 > -- Timeout interval in seconds <1-255>. **(p. 263)**

ip

- [no] interface *[ETHERNET] PORT-LIST* ip

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

- **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list (ASCII-STR) **(p. 201)**

- [no] interface *[ETHERNET] PORT-LIST* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:

- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 201)**

- [no] interface *[ETHERNET] PORT-LIST* rate-limit ip

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

- **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list**(p. 201)**

- [no] interface loopback *< 0 to 7 >* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the Loopback. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a Loopback context command. It can be called directly
             from the Loopback context or follow the 'interface loopback
             <num>' command.
```

Next Available Options:

- **address** -- Set IP parameters for communication within an IP network**(p. 203)**
- **ospf** -- configure Open Shortest Path First (OSPF) protocol parameters on the interface**(p. 243)**

- interface vlan *VLAN-ID* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the VLAN. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 201)**
- **address** -- Set IP parameters for communication within an IP network**(p. 203)**
- **proxy-arp** -- Enable/disable proxy ARP**(p. 254)**

- **local-proxy-arp** -- Enable/disable local proxy ARP**(p. 234)**
- **helper-address** -- Add or remove a DHCP server IP address for the VLAN (IP-ADDR) **(p. 223)**
- **forward-protocol** -- Add or remove a UDP server address for the VLAN**(p. 221)**
- **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature on a VLAN**(p. 224)**
- **irdp** -- Configure ICMP Router Discovery Protocol (IRDP)**(p. 231)**
- **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the VLAN interface**(p. 243)**
- **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the VLAN interface**(p. 259)**
- **pim-dense** -- Enable/disable/configure PIM-DM protocol on the VLAN interface**(p. 245)**
- **pim-sparse** -- Enable/disable/configure PIM-SM protocol on the VLAN interface**(p. 246)**
- **mroute** -- Configure IP Multicast Routing parameters on the VLAN interface**(p. 242)**

- [no] interface vlan *VLAN-ID* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:

- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 201)**

- interface svlan *VLAN-ID* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the VLAN. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 201)**
- **address** -- Set IP parameters for communication within an IP network**(p. 203)**

- [no] interface svlan *VLAN-ID* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:

- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 201)**

ip-addr

- [no] interface loopback *< 0 to 7 >* ip address *IP-ADDR*

```
Interface IP address.
```

- [no] interface loopback *< 0 to 7 >* ip ospf *IP-ADDR*

```
Specify the IP address the request is for.
```

Next Available Options:

- **area** -- Specify an OSPF area.**(p. 209)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 216)**

- [no] interface vlan *VLAN-ID* ip address *IP-ADDR/MASK-LENGTH*

  ```
  Interface IP address/mask.
  ```

- [no] interface vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR*

  ```
  IP address of the protocol server.
  ```

Next Available Options:

- **port-num** -- UDP port number of the server. (TCP/UDP-PORT) **(p. 249)**
- **port-name** < dns | ntp | netbios-ns | ... > -- (NUMBER) **(p. 249)**

- [no] interface vlan *VLAN-ID* ip ospf *IP-ADDR*

  ```
  Specify the IP address the request is for.
  ```

Next Available Options:

- **passive** -- Configures an ospf interface as passive. **(p. 245)**
- **area** -- Specify an OSPF area.**(p. 209)**
- **authentication-key** -- Set simple authentication method and key.**(p. 211)**
- **authentication** -- Disable authentication.**(p. 210)**
- **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 235)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 216)**
- **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 216)**
- **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 222)**
- **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 251)**
- **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 259)**
- **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 263)**

- [no] interface vlan *VLAN-ID* ip rip *IP-ADDR*

  ```
  Specify the IP address the request is for.
  ```

Next Available Options:

- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 212)**
- **authentication-key** -- Set RIP authentication key (maximum 16 characters).**(p. 211)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 235)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 248)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 258)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 260)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 260)**

- interface vlan *VLAN-ID* ip pim-dense ip-addr

  ```
  Usage: ip pim-dense [ip-addr IP-ADDR|any]
  ```

```
Description: Set the source IP address for the PIM-DM packets sent out on this
             interface. You can either explicitly specify one of the existing
             VLAN's IP addresses or use 'any' option to dynamically determine
             it from the VLAN's current IP configuration. The default is 'any'.
             This command also enable the PIM-DM protocol on the VLAN interface.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 227)**
- **any** -- Dynamically determine IP address.**(p. 209)**

- interface vlan *VLAN-ID* ip pim-dense ip-addr *IP-ADDR*

```
Specify IP address.
```

- interface vlan *VLAN-ID* ip pim-sparse ip-addr

```
Usage: ip pim-sparse [ip-addr IP-ADDR|any]

Description: Set the source IP address for the PIM-SM packets sent out on this
             interface. You can either explicitly specify one of the existing
             VLAN's IP addresses or use 'any' option to dynamically determine
             it from the VLAN's current IP configuration. The default is 'any'.
             This command also enable the PIM-SM protocol on the VLAN interface.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 227)**
- **any** -- Dynamically determine IP address.**(p. 209)**

- interface vlan *VLAN-ID* ip pim-sparse ip-addr *IP-ADDR*

```
Specify IP address.
```

- [no] interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* virtual-ip-address *IP-ADDR/MASK-LENGTH*

```
Specify IP address/mask.
```

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address *IP-ADDR*

```
Specify IP address.
```

- [no] interface svlan *VLAN-ID* ip address *IP-ADDR/MASK-LENGTH*

```
Interface IP address/mask.
```

ip-recv-mac-address

- [no] interface vlan *VLAN-ID* ip-recv-mac-address

```
Usage: [no] ip-recv-mac-address <macaddress> interval <1-255>

Description:  Associates a L3-mac-address with a VLAN.
      To associate L3-Mac-Address for a VLAN.
         ip-recv-mac-address <mac-address> interval <1-255>
      To associate L3-Mac-Address with a VLAN with default
      timeout interval of 60s.
         ip-recv-mac-address <mac-address>
      To disassociate L3-Mac_address with a VLAN.
             no ip-recv-mac-address
```

```
Parameters:
       <mac-address>  -  The L3-mac-address to be associated with a VLAN.
       interval       -  Specify L3-Mac-Address timeout interval.
       <1-255>        -  Timeout interval in seconds <1-255>.
```

Next Available Option:

- **mac-address** -- The L3-mac-address to be associated with a VLAN. (MAC-ADDR) **(p. 234)**

ipv6

- interface vlan *VLAN-ID* ipv6

```
Usage: [no] ipv6 ...

Description: Configure various IP parameters for the VLAN. The 'ipv6'
             command must be followed by a feature-specific keyword.
             Use 'ipv6 ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr.**(p. 219)**
- **address** -- Set IPv6 parameters for communication within an IP network**(p. 203)**
- **mld** -- Enable/disable/configure IPv6 Multicast Listener Discovery (MLD) feature on a VLAN**(p. 237)**

- interface svlan *VLAN-ID* ipv6

```
Usage: [no] ipv6 ...

Description: Configure various IP parameters for the VLAN. The 'ipv6'
             command must be followed by a feature-specific keyword.
             Use 'ipv6 ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr.**(p. 219)**
- **address** -- Set IPv6 parameters for communication within an IP network**(p. 203)**

ipv6-addr

- [no] interface vlan *VLAN-ID* ipv6 address *IPV6-ADDR*

```
Configure a link-local IPv6 address.
```

Next Available Option:

- **link-local** -- Configure a link-local IPv6 address.**(p. 234)**

- [no] interface svlan *VLAN-ID* ipv6 address *IPV6-ADDR*

  ```
  Configure a link-local IPv6 address.
  ```

  Next Available Option:

  - **link-local** -- Configure a link-local IPv6 address.**(p. 234)**

ipv6-addr/mask

- [no] interface vlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN*

  ```
  Configure IPv6 address represented in CIDR notation.
  ```

  Next Available Options:

  - **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes**(p. 209)**
  - **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface**(p. 219)**

- [no] interface svlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN*

  ```
  Configure IPv6 address represented in CIDR notation.
  ```

  Next Available Options:

  - **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes**(p. 209)**
  - **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface**(p. 219)**

irdp

- [no] interface vlan *VLAN-ID* ip irdp

  ```
  Usage: [no] ip irdp [...]

  Description: Configure ICMP Router Discovery Protocol (IRDP). This is
               a VLAN context command. It can be called directly from the VLAN
               context or may follow the 'vlan VLAN-ID' command prefix.
               Called without parameters the command enables or disables (if
               preceded by 'no') the protocol on the VLAN specified, or
               identified by the current VLAN context. Use 'ip irdp ?' to get
               a list of all possible configurable parameters.
  ```

  Next Available Options:

  - **advert-address** < multicast | broadcast > -- Specify the destination address to be used for router advertisements**(p. 206)**
  - **holdtime** < 4 to 9000 > -- Set the lifetime (in seconds) of the router advertisements sent on this interface**(p. 223)**
  - **maxadvertinterval** < 4 to 1800 > -- Set the maximum time (in seconds) allowed between sending unsolicited router advertisements**(p. 235)**
  - **minadvertinterval** < 3 to 1800 > -- Set the minimum time (in seconds) allowed between sending unsolicited router advertisements**(p. 236)**
  - **preference** -- The preferability of the router as a default router, relative to the other routers on the same subnet**(p. 250)**

join-timer

- interface *[ETHERNET] PORT-LIST* gvrp join-timer *< 20 to 75 >*

  ```
  Set join timer value (centiseconds; default 20).
  ```

  Range: < 20 to 75 >

jumbo

- [no] interface vlan *VLAN-ID* jumbo

  ```
  Usage: [no] jumbo

  Description: Labels this VLAN as a Jumbo VLAN, allowing you to pass
               packets up to 9220 bytes in size.
               This is a VLAN context command. It can be called directly
               from the VLAN context or follow the 'vlan VLAN-ID'
               command.
  ```

- [no] interface svlan *VLAN-ID* jumbo

  ```
  Usage: [no] jumbo

  Description: Labels this VLAN as a Jumbo VLAN, allowing you to pass
               packets up to 9220 bytes in size.
               This is a VLAN context command. It can be called directly
               from the VLAN context or follow the 'vlan VLAN-ID'
               command.
  ```

kbps

- interface *[ETHERNET] PORT-LIST* rate-limit icmp kbps *< 0 to 10000000 >*

  ```
  Specify kilobits-per-second limit of allowed ICMP traffic (values should be at least
   13Kbps, or max-length ICMP packets will fail.)
  ```

  Range: < 0 to 10000000 >
- interface *[ETHERNET] PORT-LIST* rate-limit all in kbps *< 0 to 10000000 >*

  ```
  Specify limit of allowed inbound or outbound traffic in kilobits-per-second on the
  specified port(s). Actual limits are in steps of 100Kbps to 100Mbps (granularity is
  1% of the lowest related media speed).
  ```

  Range: < 0 to 10000000 >
- interface *[ETHERNET] PORT-LIST* rate-limit all out kbps *< 0 to 10000000 >*

  ```
  Specify limit of allowed inbound or outbound traffic in kilobits-per-second on the
  specified port(s). Actual limits are in steps of 100Kbps to 100Mbps (granularity is
  1% of the lowest related media speed).
  ```

  Range: < 0 to 10000000 >
- interface *[ETHERNET] PORT-LIST* rate-limit ip access-group *ACCESS-GROUP < in >* kbps *< 1 to 10000000 >*

  ```
  Specify rate-limit in kilo-bits-per-second.
  ```

  Range: < 1 to 10000000 >

lacp

- [no] interface *[ETHERNET] PORT-LIST* lacp

```
Usage: [no] lacp [active|passive]

Description: Define whether LACP is enabled on the port, and whether it is in
             active or passive mode when enabled.
             When LACP is enabled and active, the port will both send LACP
             packets and listen to them.
             When LACP is enabled and passive, the port will send LACP packets
             only if it is spoken to.
             When LACP is disabled, the port will ignore LACP packets.
             If 'lacp' command is issued without a mode parameter, 'active' is
             assumed.
             With 'no lacp' the mode parameter is not allowed.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Next Available Option:

- **mode** < Active | Passive > -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled**(p. 238)**

lan-prune-delay

- [no] interface vlan *VLAN-ID* ip pim-dense lan-prune-delay

```
Usage: [no] ip pim-dense lan-prune-delay

Description: Turn on/off the LAN Prune Delay Option on this interface.
             Default is 'on'.
```

- [no] interface vlan *VLAN-ID* ip pim-sparse lan-prune-delay

```
Usage: [no] ip pim-sparse lan-prune-delay

Description: Turn on/off the LAN Prune Delay Option on this interface.
             Default is 'on'.
```

leaveall-timer

- interface *[ETHERNET] PORT-LIST* gvrp leaveall-timer *< 500 to 3000 >*

```
Set leaveall timer value (centiseconds; default 1000).
```

Range: < 500 to 3000 >

leave-timer

- interface *[ETHERNET] PORT-LIST* gvrp leave-timer *< 40 to 300 >*

```
Set leave timer value (centiseconds; default 300).
```

Range: < 40 to 300 >

link-keepalive

- [no] interface *[ETHERNET] PORT-LIST* link-keepalive

```
Usage: [no]link-keepalive [vlan <vlan-id>]

Description: Configure UDLD on port(s).
             The command enables/disables UDLD on particular port/port-list
```

```
By default UDLD control packets are untagged.
The user has to give vlan-id for tagged UDLD control packets.
```

Next Available Option:

- **vlan** -- Set vlan-id for tagged UDLD control packets. (VLAN-ID) **(p. 266)**

link-local

- [no] interface vlan *VLAN-ID* ipv6 address *IPV6-ADDR* link-local

```
Configure a link-local IPv6 address.
```

- [no] interface svlan *VLAN-ID* ipv6 address *IPV6-ADDR* link-local

```
Configure a link-local IPv6 address.
```

local-proxy-arp

- [no] interface vlan *VLAN-ID* ip local-proxy-arp

```
Usage: [no] ip local-proxy-arp

Description: Enable/disable local proxy ARP. This is a VLAN context command.
             It can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix. When local proxy ARP is
             enabled on a VLAN, the device responds to all ARP requests
             received on the VLAN ports with it's own hardware address.
```

loopback

- [no] interface loopback *< 0 to 7 >*

```
Usage: [no] interface loopback <num>

Description: Enter the loopback Configuration Level.
```

Range: < 0 to 7 >

Next Available Option:

- **ip** -- Configure various IP parameters for the Loopback**(p. 225)**

lowest

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address lowest

```
Dynamically determine lowest IP address.
```

mac-address

- interface vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR*

```
The L3-mac-address to be associated with a VLAN.
```

Next Available Option:

- **interval** -- Specify the L3-Mac-Address timeout interval. **(p. 225)**

maxadvertinterval

- interface vlan *VLAN-ID* ip irdp maxadvertinterval *< 4 to 1800 >*

```
Usage: [no] ip irdp maxadvertinterval <4-1800>

Description: Set the maximum time (in seconds) allowed between sending
             unsolicited router advertisements.
```

Range: < 4 to 1800 >

max-graft-retries

- interface vlan *VLAN-ID* ip pim-dense max-graft-retries *< 1 to 10 >*

```
Usage: ip pim-dense max-graft-retries <1-10>

Description: Set the maximum number of times this router will resend a
             Graft on this interface. Default is 2.
```

Range: < 1 to 10 >

md5-auth-key-chain

- interface vlan *VLAN-ID* ip ospf md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 215)**

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 215)**

- interface vlan *VLAN-ID* ip ospf all md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 215)**

mdix-mode

- interface *[ETHERNET] PORT-LIST* mdix-mode *< mdi | mdix | autoMDIX >*

```
Set port MDI/MDIX mode (default: auto).
```

Supported Values:

- **mdi** -- Configures port for connecting a PC with a crossover cable
- **mdix** -- Configures port for connecting a PC with a straight-through cable
- **autoMDIX** -- Configures port for automatic detection of the cable

metric

- interface vlan *VLAN-ID* ip rip metric *< 1 to 15 >*

```
Set metric for this interface.
```

Range: < 1 to 15 >

- interface vlan *VLAN-ID* ip rip *IP-ADDR* metric *< 1 to 15 >*

```
Set metric for this interface.
```

Range: < 1 to 15 >

- interface vlan *VLAN-ID* ip rip all metric *< 1 to 15 >*

```
Set metric for this interface.
```

Range: < 1 to 15 >

minadvertinterval

- interface vlan *VLAN-ID* ip irdp minadvertinterval *< 3 to 1800 >*

```
Usage: [no] ip irdp minadvertinterval <3-1800>

Description: Set the minimum time (in seconds) allowed between sending
             unsolicited router advertisements. Must be no greater than the
             maximum time between sending unsolicited router advertisements.
```

Range: < 3 to 1800 >

mirror

- interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >* mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 241)**
- **mirror_session_name** -- Mirror destination name.**(p. 237)**

- interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP* *< In >* mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 241)**
- **mirror_session_name** -- Mirror destination name.**(p. 237)**

- interface vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 241)**
- **mirror_session_name** -- Mirror destination name.**(p. 237)**

- interface vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 241)**
- **mirror_session_name** -- Mirror destination name.**(p. 237)**

- interface svlan *VLAN-ID* monitor all < *In* | *Out* | *Both* > mirror

  ```
  Mirror destination.
  ```

  Next Available Options:

  - **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 241)**
  - **mirror_session_name** -- Mirror destination name.**(p. 237)**

- interface svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* < *In* > mirror

  ```
  Mirror destination.
  ```

  Next Available Options:

  - **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 241)**
  - **mirror_session_name** -- Mirror destination name.**(p. 237)**

mirror_session_name

- [no] interface *[ETHERNET] PORT-LIST* monitor all < *In* | *Out* | *Both* > mirror

  ```
  Mirror destination name.
  ```

- [no] interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP* < *In* > mirror

  ```
  Mirror destination name.
  ```

- [no] interface vlan *VLAN-ID* monitor all < *In* | *Out* | *Both* > mirror

  ```
  Mirror destination name.
  ```

- [no] interface vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* < *In* > mirror

  ```
  Mirror destination name.
  ```

- [no] interface svlan *VLAN-ID* monitor all < *In* | *Out* | *Both* > mirror

  ```
  Mirror destination name.
  ```

- [no] interface svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* < *In* > mirror

  ```
  Mirror destination name.
  ```

mld

- [no] interface vlan *VLAN-ID* ipv6 mld

  ```
  Usage: [no] ipv6 mld [...]

  Description: Enable/disable/configure IPv6 Multicast Listener Discovery (MLD)
               feature on a VLAN.  This command enables, disables or
               configures the MLD feature for MLD communication between
               Multicast Routers, Multicast Servers, and Multicast Clients
               connected to the device.  This is a VLAN context command.
  ```

```
                If not preceded by 'no',
                the command accepts a variety of configuration parameters. To
                get a list of all available parameters use 'ipv6 mld ?'. To
                get detailed help for a parameter follow it with 'help'
                keyword.
```

Next Available Options:

- **querier** -- This command disables or re-enables the ability for the switch to become querier if necessary**(p. 255)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 212)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 214)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 221)**
- **fastleave** -- Enables MLD fast-leaves on the specified ports in the selected VLAN ([ethernet] PORT-LIST) **(p. 219)**
- **forcedfastleave** -- Enables MLD Forced Fast-Leave on the specified ports in the selected VLAN, even if they are cascaded ([ethernet] PORT-LIST) **(p. 220)**

mode

- interface *[ETHERNET] PORT-LIST* lacp *< Active* | *Passive >*

```
Usage: [no] lacp [active|passive]

Description: Define whether LACP is enabled on the port, and whether it is in
             active or passive mode when enabled.
             When LACP is enabled and active, the port will both send LACP
             packets and listen to them.
             When LACP is enabled and passive, the port will send LACP packets
             only if it is spoken to.
             When LACP is disabled, the port will ignore LACP packets.
             If 'lacp' command is issued without a mode parameter, 'active' is
             assumed.
             With 'no lacp' the mode parameter is not allowed.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Supported Values:

- **Active** -- Enable active LACP.
- **Passive** -- Enable passive LACP.

monitor

- [no] interface *[ETHERNET] PORT-LIST* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
              [1-4 | NAME-STR]...
          [no] monitor ip access-group <ACL-NAME> <in> mirror
              <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the port is to be monitored or not.
             The network traffic seen by the monitored ports is copied to
             the Mirroring Destination to which a network analyzer can be
             attached.
             Note: When mirroring multiple ports in a busy network,
             some frames may not be copied to the mirroring port.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.

Parameters:     o 1-4 - Mirror destination number
             o NAME-STR - Friendly name associated with the mirror
             destination number.
             o ACL-NAME - Standard or Extended Access Control List number.
             o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 207)**
- **ip** -- Apply an IPv4 access list.**(p. 225)**

- [no] interface vlan *VLAN-ID* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
                 [1-4 | NAME-STR]...
       2) [no] monitor ip access-group <ACL-NAME> <in> mirror
                <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the VLAN is to be monitored or not.
                The network traffic seen by the monitored VLAN is copied to
                the Mirroring Destination to which a network analyzer can be
                attached.
                Note: When mirroring a VLAN in a busy network,
                some frames may not be copied to the mirroring port.
                This is an VLAN context command. It can be called directly
                from the VLAN context or follow the 'vlan VLAN-ID command.

Parameters:     o 1-4 - Mirror destination number
                o NAME-STR - Friendly name associated with the mirror
                destination number.
                o ACL-NAME - Standard or Extended Access Control List number.
                o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 207)**
- **ip** -- Apply an IPv4 access list.**(p. 225)**

- [no] interface svlan *VLAN-ID* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
                 [1-4 | NAME-STR]...
       2) [no] monitor ip access-group <ACL-NAME> <in> mirror
                <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the VLAN is to be monitored or not.
                The network traffic seen by the monitored VLAN is copied to
                the Mirroring Destination to which a network analyzer can be
                attached.
                Note: When mirroring a VLAN in a busy network,
                some frames may not be copied to the mirroring port.
                This is an VLAN context command. It can be called directly
                from the VLAN context or follow the 'vlan VLAN-ID command.
```

```
Parameters:  o 1-4 - Mirror destination number
             o NAME-STR - Friendly name associated with the mirror
             destination number.
             o ACL-NAME - Standard or Extended Access Control List number.
             o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 207)**
- **ip** -- Apply an IPv4 access list.**(p. 225)**

monitor_mirror_ACL_dir

- interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP < In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 236)**

- interface vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP < In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 236)**

- interface svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 236)**

monitor_mirror_session_id

- [no] interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] interface vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] interface vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] interface svlan *VLAN-ID* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] interface svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

mroute

- interface vlan *VLAN-ID* ip mroute

```
Usage: ip mroute ...

Description: Configure IP Multicast Routing parameters on the VLAN
             interface. The command must be followed by a parameter.
             Use 'ip mroute ?' to get a list of all possible parameters.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **ttl-threshold** < 0 to 255 > -- Set the multicast datagram TTL threshold for the interface**(p. 264)**

name

- [no] interface *[ETHERNET] PORT-LIST* name

```
Usage:    name PORT-NAME-STR
       no name

Description: Set/unset a name for the port(s).
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Next Available Option:

- **port-name** -- Specify a port name up to 64 characters length. (ASCII-STR) **(p. 249)**

- interface vlan *VLAN-ID* name *NAME*

```
Usage: name ASCII-STR

Description: Set the VLAN's name.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- interface svlan *VLAN-ID* name *NAME*

```
Usage: name ASCII-STR

Description: Set the VLAN's name.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

nbr-timeout

- interface vlan *VLAN-ID* ip pim-sparse nbr-timeout *< 60 to 8000 >*

```
Usage: ip pim-sparse nbr-timeout <60-8000>

Description: Set the neighbour loss time interval for this interface.
             Default is 180 seconds.
```

Range: < 60 to 8000 >

no-default

- interface vlan *VLAN-ID* ip irdp preference no-default

```
Indicates that the router should never be used as a default by its neighbors.
```

number

- interface vlan *VLAN-ID* ip irdp preference *< -2147483647 to 2147483647 >*

```
The router preferability number. Higher values are more preferable.
```

Range: < -2147483647 to 2147483647 >

ospf

- [no] interface loopback *< 0 to 7 >* ip ospf

```
Usage: [no] ip ospf [...]

Description: configure Open Shortest Path First (OSPF)
             protocol parameters on the interface.
             Called without 'no', the command configures OSPF parameter on
             interface. Otherwise ('no' is specified), the command remove
             specified ospf parameter on the interface. Use 'ip ospf ?' to
             get a list of all possible options.
```

Next Available Options:

- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 227)**
- **all** -- Process the request for all IP addresses.**(p. 207)**

- [no] interface vlan *VLAN-ID* ip ospf

```
Usage: [no] ip ospf [...]

Description: Enable/disable/configure Open Shortest Path First (OSPF)
             protocol on the VLAN interface.
             Called without 'no', the command enables OSPF on the interface.
             Otherwise ('no' is specified), the command disables OSPF on the
             interface. The command can be followed by an OSPF configuration
             command. Use 'ip ospf ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **passive** -- Configures an ospf interface as passive. **(p. 245)**
- **area** -- Specify an OSPF area.**(p. 209)**
- **authentication-key** -- Set simple authentication method and key.**(p. 211)**
- **authentication** -- Disable authentication.**(p. 210)**
- **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 235)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 216)**

- **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 216)**
- **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 222)**
- **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 251)**
- **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 259)**
- **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 263)**
- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 227)**
- **all** -- Process the request for all IP addresses.**(p. 207)**

out

- [no] interface *[ETHERNET] PORT-LIST* rate-limit all out

```
Set limits for all outbound traffic.
```

Next Available Options:

- **percent** < 0 to 100 > -- Specify limit as percent of inbound or outbound traffic.**(p. 245)**
- **kbps** < 0 to 10000000 > -- Specify limit of allowed inbound or outbound traffic in kilobits-per-second on the specified port(s). Actual limits are in steps of 100Kbps to 100Mbps (granularity is 1% of the lowest related media speed). **(p. 232)**

output

- [no] interface *[ETHERNET] PORT-LIST* bandwidth-min output

```
Enable/disable and configure guaranteed minimum bandwidth for outgoing traffic.
```

Next Available Option:

- **queue1** < 0 to 100 > -- Specify min. bandwidth percentage for queue one outgoing traffic.**(p. 256)**

override-interval

- interface vlan *VLAN-ID* ip pim-dense override-interval *< 500 to 6000 >*

```
Usage: ip pim-dense override-interval <500-6000>

Description: Set the value inserted into the Override Interval field of
             a LAN Prune Delay option on this interface. Default is 2500
             milliseconds.
```

Range: < 500 to 6000 >

- interface vlan *VLAN-ID* ip pim-sparse override-interval *< 500 to 6000 >*

```
Usage: ip pim-sparse override-interval <500-6000>

Description: Set the value inserted into the Override Interval field of
             a LAN Prune Delay option on this interface. Default is 2500
             milliseconds.
```

Range: < 500 to 6000 >

owner

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* owner

```
Usage: vrrp vrid <VRID> owner

Description: Designate the virtual router instance as an Owner (Master).
             There is no default value.
```

passive

- [no] interface vlan *VLAN-ID* ip ospf passive

```
Configures an ospf interface as passive.
```

- [no] interface vlan *VLAN-ID* ip ospf *IP-ADDR* passive

```
Configures an ospf interface as passive.
```

- [no] interface vlan *VLAN-ID* ip ospf all passive

```
Configures an ospf interface as passive.
```

percent

- interface *[ETHERNET] PORT-LIST* rate-limit icmp percent *< 0 to 100 >*

```
Specify limit as percent of inbound or outbound traffic.
```

Range: < 0 to 100 >

- interface *[ETHERNET] PORT-LIST* rate-limit all in percent *< 0 to 100 >*

```
Specify limit as percent of inbound or outbound traffic.
```

Range: < 0 to 100 >

- interface *[ETHERNET] PORT-LIST* rate-limit all out percent *< 0 to 100 >*

```
Specify limit as percent of inbound or outbound traffic.
```

Range: < 0 to 100 >

pim-dense

- [no] interface vlan *VLAN-ID* ip pim-dense

```
Usage: [no] ip pim-dense [...]

Description: Enable/disable/configure PIM-DM protocol on the VLAN interface.
             Use direct and 'no' versions of the command to enable/disable
             PIM-DM on the interface. Use 'ip pim-dense ?' to get the list
             of all configuration options. This command can be used in the
             VLAN context or in the global context with the 'vlan <VLAN-ID>'
             prefix.
```

Next Available Options:

- **ip-addr** -- Set the source IP address for the PIM-DM packets sent out on this interface**(p. 227)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface**(p. 233)**
- **hello-interval** < 5 to 300 > -- Set the frequency at which PIM Hello messages are transmitted on this interface**(p. 222)**
- **hello-delay** < 0 to 5 > -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface**(p. 222)**
- **graft-retry-interval** < 1 to 10 > -- Set the interval a PIM router waits for a Graft Ack before resending a Graft on this interface**(p. 222)**

- **max-graft-retries** < 1 to 10 > -- Set the maximum number of times this router will resend a Graft on this interface**(p. 235)**
- **override-interval** < 500 to 6000 > -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface**(p. 244)**
- **propagation-delay** < 250 to 2000 > -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface**(p. 252)**
- **ttl-threshold** < 0 to 255 > -- Set the Time To Live in a PIM-DM State Refresh message at which it is not forwarded on this interface**(p. 264)**

pim-sparse

- [no] interface vlan *VLAN-ID* ip pim-sparse

```
Usage: [no] ip pim-sparse [...]

Description: Enable/disable/configure PIM-SM protocol on the VLAN interface.
             Use direct and 'no' versions of the command to enable/disable
             PIM-SM on the interface. Use 'ip pim-sparse ?' to get the list
             of all configuration options. This command can be used in the
             VLAN context or in the global context with the 'vlan <VLAN-ID>'
             prefix.
```

Next Available Options:

- **ip-addr** -- Set the source IP address for the PIM-SM packets sent out on this interface**(p. 227)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface**(p. 233)**
- **hello-interval** < 5 to 300 > -- Set the frequency at which PIM Hello messages are transmitted on this interface**(p. 222)**
- **hello-delay** < 0 to 5 > -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface**(p. 222)**
- **override-interval** < 500 to 6000 > -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface**(p. 244)**
- **propagation-delay** < 250 to 2000 > -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface**(p. 252)**
- **dr-priority** -- Set the priority value to use on the interface in the Designated Router election process**(p. 218)**
- **nbr-timeout** < 60 to 8000 > -- Set the neighbour loss time interval for this interface**(p. 242)**

poe_lldp_detect

- interface *[ETHERNET] PORT-LIST* poe-lldp-detect *< disabled | enabled >*

```
Usage: poe-lldp-detect [disabled|enabled]

Description: Enabling this feature causes the port to allocate power
             based on the link-partner's capabilities via LLDP.
             By default, poe information detected though LLDP
             are ignored as not all PoE devices properly support LLDP.
```

Supported Values:

- **disabled**
- **enabled**

poe_value

- interface *[ETHERNET] PORT-LIST* poe-value *< 1 | 2 | 3 | ... >*

```
Usage: poe-value [1-17]

Description: Maximum PoE allocation specified with a value in watts.
             By default, power-over-ethernet allocation is automatic by
             usage of the powered device with a maximum set at 17W
             This can be changed so the POE allocation is fixed at
             whatever poe-value is set to and by setting the port
             allocation to be by value using: poe-allocate-by value.
```

Supported Values:

- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**
- **11**
- **12**
- **13**
- **14**
- **15**
- **16**
- **17**

poe-allocate-by

- interface *[ETHERNET] PORT-LIST* poe-allocate-by

```
Usage: poe-allocate-by [usage|class|value]

Description: Control manual power over ethernet allocation.
             By default, power-over-ethernet allocation is automatic by
             usage of the powered device. This can be overriden by manually
             specifying how much power this port should be allocated by
             either its class or a user-defined value.
```

Next Available Option:

- **allocate_by** < usage | class | value > -- Control manual power over ethernet allocation**(p. 208)**

poe-lldp-detect

- interface *[ETHERNET] PORT-LIST* poe-lldp-detect

```
Usage: poe-lldp-detect [disabled|enabled]

Description: Enabling this feature causes the port to allocate power
             based on the link-partner's capabilities via LLDP.
             By default, poe information detected though LLDP
             are ignored as not all PoE devices properly support LLDP.
```

Next Available Option:

- **poe_lldp_detect** < disabled | enabled > -- Enabling this feature causes the port to allocate power based on the link-partner's capabilities via LLDP**(p. 246)**

poe-value

- interface *[ETHERNET] PORT-LIST* poe-value

```
Usage: poe-value [1-17]

Description: Maximum PoE allocation specified with a value in watts.
             By default, power-over-ethernet allocation is automatic by
             usage of the powered device with a maximum set at 17W
             This can be changed so the POE allocation is fixed at
             whatever poe-value is set to and by setting the port
             allocation to be by value using: poe-allocate-by value.
```

Next Available Option:

- **poe_value** < 1 | 2 | 3 | ... > -- Maximum PoE allocation specified with a value in watts**(p. 246)**

poison-reverse

- [no] interface vlan *VLAN-ID* ip rip poison-reverse

```
Enable/disable poison reverse on this interface.
```

- [no] interface vlan *VLAN-ID* ip rip *IP-ADDR* poison-reverse

```
Enable/disable poison reverse on this interface.
```

- [no] interface vlan *VLAN-ID* ip rip all poison-reverse

```
Enable/disable poison reverse on this interface.
```

port-list

- interface *[ETHERNET] PORT-LIST*

```
Usage: [no] interface [ethernet] PORT-LIST [...]

Description: Enter the Interface Configuration Level, or execute one
             command for that level. Without optional parameters
             specified, the 'interface' command changes the context to
             the Interface Configuration Context Level for execution of
             configuration changes to the port or ports in the PORT-LIST.
             The 'interface [ethernet] PORT-LIST' can be followed by any
             command from the Interface Configuration Context Level in the
             same command line. In this case the context level is not
             changed, but the command is also executed for the port or ports
             in the PORT-LIST. Use 'interface [ethernet] PORT-LIST ?'
             to get a list of all valid commands.
```

Next Available Options:

- **ip** -- Apply the specified access control list to inbound packets on this INTERFACE list**(p. 225)**
- **broadcast-limit** < 0 to 99 > -- Set a broadcast traffic percentage limit**(p. 215)**
- **dhcp-snooping** -- Configure the port as trusted or untrusted**(p. 217)**
- **disable** -- Disable port(s)**(p. 218)**
- **enable** -- Enable port(s)**(p. 219)**
- **flow-control** -- Enable/disable flow control on the port(s)**(p. 220)**
- **gvrp** -- Set the GVRP timers on the port (hundredths of a second)**(p. 222)**

- **lacp** -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled**(p. 232)**
- **mdix-mode** < mdi | mdix | autoMDIX > -- Set port MDI/MDIX mode (default: auto).**(p. 235)**
- **monitor** -- Define either the port is to be monitored or not**(p. 238)**
- **name** -- Set/unset a name for the port(s)**(p. 242)**
- **power-over-ethernet** -- Enable/Disable per-port power distribution**(p. 250)**
- **poe-allocate-by** -- Control manual power over ethernet allocation**(p. 247)**
- **poe-value** -- Maximum PoE allocation specified with a value in watts**(p. 248)**
- **poe-lldp-detect** -- Enabling this feature causes the port to allocate power based on the link-partner's capabilities via LLDP**(p. 247)**
- **qos** -- Set port-based priority**(p. 254)**
- **speed-duplex** < 10-half | 100-half | 10-full | ... > -- Define mode of operation for the port(s)**(p. 261)**
- **type** < Trunk | | | ... > -- **(p. 264)**
- **unknown-vlans** < Learn | Block | Disable > -- Configure GVRP on the port(s)**(p. 265)**
- **bandwidth-min** -- Enable/disable and configure guaranteed minimum bandwidth settings for outgoing traffic on the port(s)**(p. 214)**
- **rate-limit** -- Enable/disable and configure rate-limiting for all traffic (or for incoming ICMP traffic) on the port(s)**(p. 258)**
- **link-keepalive** -- Configure UDLD on port(s)**(p. 233)**
- **arp-protect** -- Configure the port as trusted or untrusted**(p. 210)**
- **qinq** -- Configure a port's type as customer-network or provider-network**(p. 254)**

port-name

- interface *[ETHERNET] PORT-LIST* name *PORT-NAME*

```
Specify a port name up to 64 characters length.
```

- [no] interface vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR < dns | ntp | netbios-ns | ... >*

  Supported Values:
  - **dns** -- Domain Name Service (53)
  - **ntp** -- Network Time Protocol (123)
  - **netbios-ns** -- NetBIOS Name Service (137)
  - **netbios-dgm** -- NetBIOS Datagram Service (138)
  - **radius** -- Remote Authentication Dial-In User Service (1812)
  - **radius-old** -- Remote Authentication Dial-In User Service (1645)
  - **rip** -- Routing Information Protocol (520)
  - **snmp** -- Simple Network Management Protocol (161)
  - **snmp-trap** -- Simple Network Management Protocol (162)
  - **tftp** -- Trivial File Transfer Protocol (69)
  - **timep** -- Time Protocol (37)

port-num

- [no] interface vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR TCP/UDP-PORT*

```
UDP port number of the server.
```

port-type

- interface *[ETHERNET] PORT-LIST* qinq port-type

```
Configure qinq port-type
```

Next Available Options:

- **customer-network** -- Configure qinq port-type as customer-network**(p. 216)**
- **provider-network** -- Configure qinq port-type as provider-network**(p. 254)**

power-over-ethernet

- [no] interface *[ETHERNET] PORT-LIST* power-over-ethernet

```
Usage: [no] power-over-ethernet [critical|high|low]

Description: Enable/Disable per-port power distribution. Specifying critical,
             high, or low indicates the priority of the port to get power in
             the event of power over-subscription. Per-port power is enabled
             by default. The default priority is low.
             Note: Lower numbered ports have precedence over higher numbered
             ports of the same priority.
```

Next Available Option:

- **priority** < critical | high | low > -- Enable/Disable per-port power distribution**(p. 251)**

preempt-delay-time

- [no] interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* preempt-delay-time *< 1 to 600 >*

```
Usage: [no] vrrp vrid <VRID> preempt-delay-time <1-600>

Description: Enable the pre-emptive delay timer for the virtual router
             instance.
             [no] may be used to disable the pre-emptive delay timer.

Parameters:

    o preempt-delay-time <1-600> - The number of seconds to delay.
```

Range: < 1 to 600 >

preempt-mode

- [no] interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* preempt-mode

```
Usage: [no] vrrp vrid <VRID> preempt-mode

Description: Enable/disable preempt mode for the virtual router instance.
             The default value is 'enabled'.
```

preference

- interface vlan *VLAN-ID* ip irdp preference

```
Usage: [no] ip irdp preference <no-default|<-2147483647-2147483647>>

Description: The preferability of the router as a default
             router, relative to the other routers on the same
             subnet.  Higher values are more preferable.
```

Next Available Options:

- **number** < -2147483647 to 2147483647 > -- The router preferability number. Higher values are more preferable.**(p. 243)**
- **no-default** -- Indicates that the router should never be used as a default by its neighbors.**(p. 243)**

primary-ip-address

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address

```
Usage: [no] vrrp vrid <VRID> primary-ip-address <IP-ADDR | lowest>

Description: Specify IP address the virtual router instance will use as
             a source in VRRP advertisement messages. If not set (i.e. is
             '0.0.0.0') the virtual router uses numerically lowest IP address
             of the VLAN. The default value is 'lowest'.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 227)**
- **lowest** -- Dynamically determine lowest IP address.**(p. 234)**

priority

- interface *[ETHERNET] PORT-LIST* power-over-ethernet *< critical | high | low >*

```
Usage: [no] power-over-ethernet [critical|high|low]

Description: Enable/Disable per-port power distribution. Specifying critical,
             high, or low indicates the priority of the port to get power in
             the event of power over-subscription. Per-port power is enabled
             by default. The default priority is low.
             Note: Lower numbered ports have precedence over higher numbered
             ports of the same priority.
```

Supported Values:

- **critical**
- **high**
- **low**

- interface *[ETHERNET] PORT-LIST* qos priority *< 0 | 1 | 2 | ... >*

```
Specify priority to use.
```

Supported Values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

- interface vlan *VLAN-ID* ip ospf priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- interface vlan *VLAN-ID* ip ospf all priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- interface vlan *VLAN-ID* qos priority *< 0 | 1 | 2 | ... >*

```
Specify priority to use.
```

Supported Values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

- interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* priority *< 1 to 255 >*

```
Usage: vrrp vrid <VRID> priority <1-255>

Description: Configure priority for the virtual router instance.
             The default value is '100'.
```

Range: < 1 to 255 >

- interface svlan *VLAN-ID* qos priority *< 0 | 1 | 2 | ... >*

```
Specify priority to use.
```

Supported Values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

propagation-delay

- interface vlan *VLAN-ID* ip pim-dense propagation-delay *< 250 to 2000 >*

```
Usage: ip pim-dense propagation-delay <250-2000>

Description: Set the value inserted into the LAN Prune Delay field of a
             LAN Prune Delay option on this interface. Default is 500
             milliseconds.
```

Range: < 250 to 2000 >

- interface vlan *VLAN-ID* ip pim-sparse propagation-delay *< 250 to 2000 >*

```
Usage: ip pim-sparse propagation-delay <250-2000>

Description: Set the value inserted into the LAN Prune Delay field of a
             LAN Prune Delay option on this interface. Default is 500
             milliseconds.
```

Range: < 250 to 2000 >

protocol

- interface vlan *VLAN-ID* protocol

  ```
  Set a predefined protocol for the current VLAN.
  ```

  Next Available Options:
  - **protocols** < IPX | IPv4 | IPv6 | ... > -- Set a predefined protocol for the current VLAN. **(p. 253)**
  - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 253)**

- interface svlan *VLAN-ID* protocol

  ```
  Set a predefined protocol for the current VLAN.
  ```

  Next Available Options:
  - **protocols** < IPX | IPv4 | IPv6 | ... > -- Set a predefined protocol for the current VLAN. **(p. 253)**
  - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 253)**

protocol-group

- [no] interface vlan *VLAN-ID* protocol *PROTOCOL-GROUP*

  ```
  Enter a list of protocols for the current VLAN delimited by commas.
  ```

- [no] interface svlan *VLAN-ID* protocol *PROTOCOL-GROUP*

  ```
  Enter a list of protocols for the current VLAN delimited by commas.
  ```

protocols

- [no] interface vlan *VLAN-ID* protocol *< IPX | IPv4 | IPv6 | ... >*

  ```
  Set a predefined protocol for the current VLAN.
  ```

  Supported Values:
  - **IPX** -- IPX Protocol Group
  - **IPv4** -- IP version 4 Protocol Group
  - **IPv6** -- IP version 6 Protocol Group
  - **ARP** -- Address Resolution Protocol Group
  - **Appletalk** -- Appletalk Protocol Group
  - **SNA** -- System Network Architecture Protocol Group
  - **NetBEUI** -- Network BIOS Enhanced User Interface Protocol Group
- [no] interface svlan *VLAN-ID* protocol *< IPX | IPv4 | IPv6 | ... >*

  ```
  Set a predefined protocol for the current VLAN.
  ```

  Supported Values:

- **IPX** -- IPX Protocol Group
- **IPv4** -- IP version 4 Protocol Group
- **IPv6** -- IP version 6 Protocol Group
- **ARP** -- Address Resolution Protocol Group
- **Appletalk** -- Appletalk Protocol Group
- **SNA** -- System Network Architecture Protocol Group
- **NetBEUI** -- Network BIOS Enhanced User Interface Protocol Group

provider-network

- interface *[ETHERNET] PORT-LIST* qinq port-type provider-network

```
Configure qinq port-type as provider-network
```

proxy-arp

- [no] interface vlan *VLAN-ID* ip proxy-arp

```
Usage: [no] ip proxy-arp

Description: Enable/disable proxy ARP. This is a VLAN context command.
             It can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix. When proxy ARP is enabled on
             a VLAN, the device responds to ARP requests received on the
             VLAN ports when the device knows a route to the requested IP
             addresses.
```

qinq

- interface *[ETHERNET] PORT-LIST* qinq

```
Usage: qinq port-type <cn-customer-network-port|pn-provider-network-port>

Description: Configure a port's type as customer-network or provider-network.
             In svlan mode, the default port type is 'provider-network'. In
             mixedvlan mode, default for SVLAN ports is 'provider-network'.
             Configuring a port as either customer-network or provider-network
             is applicable only if the device is configured in either svlan or
             mixedvlan mode.
```

Next Available Option:

- **port-type** -- Configure qinq port-type**(p. 249)**

qos

- [no] interface *[ETHERNET] PORT-LIST* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]

Description: Set port-based priority. The 'dscp' or 'priority' must be
             specified if 'no' is not used. Using 'no' configures the device
             not to apply a source-port priority to this port's packets.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 218)**

- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 251)**

- [no] interface vlan *VLAN-ID* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]

Description: Set VLAN-based priority. The 'dscp' or 'priority' must
             be specified if 'no' is not used. Using 'no' configures
             the switch not to apply a VLAN priority override to this
             VLAN's packets.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 218)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 251)**

- [no] interface svlan *VLAN-ID* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]

Description: Set VLAN-based priority. The 'dscp' or 'priority' must
             be specified if 'no' is not used. Using 'no' configures
             the switch not to apply a VLAN priority override to this
             VLAN's packets.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 218)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 251)**

querier

- [no] interface vlan *VLAN-ID* ip igmp querier

```
Usage: [no] ip igmp querier [interval <seconds>]

Description: Specify querier/non-querier capability for the VLAN. IGMP
             queries are not sent when the mode is disabled. When
             enabled, the device cannot become Querier for the subnet
             unless the VLAN has an IP Address (use the 'show ip' command
             to determine this).  Each subnet must have at least one IGMP
             Querier-capable device in order for IGMP to function
             properly.  The querier interval setting modifies the time (in
             seconds) between IGMP queries.
```

Next Available Option:

- **interval** < 5 to 300 > -- Sets the interval in seconds between IGMP queries (default: 125) **(p. 225)**

- [no] interface vlan *VLAN-ID* ipv6 mld querier

```
Usage: [no] vlan < vid > ipv6 mld querier

Description: This command disables or re-enables the ability for the switch
             to become querier if necessary. The no version of the command
             disables the querier function on the switch.
             The show ipv6 mld config command displays the current querier
             command. (Default Querier Capability: Enabled.)
```

queue1

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 >*

```
Specify min. bandwidth percentage for queue one outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue2** < 0 to 100 > -- Specify min. bandwidth percentage for queue two outgoing traffic.**(p. 256)**

queue2

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue two outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue3** < 0 to 100 > -- Specify min. bandwidth percentage for queue three outgoing traffic.**(p. 256)**

queue3

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue three outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue4** < 0 to 100 > -- Specify min. bandwidth percentage for queue four outgoing traffic.**(p. 256)**

queue4

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue four outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue5** < 0 to 100 > -- Specify min. bandwidth percentage for queue five outgoing traffic.**(p. 257)**

queue5

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue five outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue6** < 0 to 100 > -- Specify min. bandwidth percentage for queue six outgoing traffic.**(p. 257)**

queue6

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue six outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue7** < 0 to 100 > -- Specify min. bandwidth percentage for queue seven outgoing traffic.**(p. 257)**

queue7

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue seven outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue8** < 0 to 100 > -- Specify min. bandwidth percentage for queue eight outgoing traffic.**(p. 257)**

queue8

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue eight outgoing traffic.
```

Range: < 0 to 100 >

rapid-commit

- [no] interface vlan *VLAN-ID* ipv6 address dhcp full rapid-commit

```
Obtain IPv6 address quickly from DHCPv6 server.
```

- [no] interface svlan *VLAN-ID* ipv6 address dhcp full rapid-commit

```
Obtain IPv6 address quickly from DHCPv6 server.
```

rate-limit

- interface *[ETHERNET] PORT-LIST* rate-limit

```
Usage: rate-limit icmp <percent <0-100> | kbps <0-10000000>>
       rate-limit all <in|out> <percent <0-100> | kbps <0-10000000>>
       rate-limit ip access-group <acl-name> in kbps <0-10000000>
       no rate-limit <icmp| all <in|out>| ip access-group>>

Description: Enable/disable and configure rate-limiting for all traffic
             (or for incoming ICMP traffic) on the port(s). By default,
             rate-limiting is disabled on all ports. When a port is
             configured to rate-limit traffic, it forwards only that
             specified amount of traffic (percentage, bits-per-second, or
             kilobits-per-second). The remaining over-profile traffic of the
             type being rate-limited is then discarded.

             Rate-Limiting works on inbound ICMP traffic, or on inbound or
             outbound traffic in general. The rate-limit reflects the
             permitted forwarding rate of the traffic type. It is visible as
             the average rate of the outbound traffic (or outbound ICMP
             traffic) originating from the rate-limited port (when in inbound
             mode), or as the average rate of the outbound traffic from an
             outbound rate-limited port.

             Rate-limiting of all traffic is primarily used for end-node
             connections (i.e., at the network edge). It is not recommended
             for use on links to servers, routers, switches, or the network
             backbone or core.
             (Rate-limiting all traffic on such links can interfere with
             important network functions.)

             ICMP rate-limiting is primarily used for throttling worm or virus-
             like behavior, and should NOT be used to remove all ICMP traffic
             from the network, as this protocol is necessary for routing
             functions.

             For more detailed information on rate-limiting, please consult
             the product manual.

             This is an Interface context command. It can be called directly
             from the interface context, or following the
             'interface [ethernet] PORT-LIST' command.
```

Next Available Options:

- **icmp** -- Set limits for ICMP traffic only.**(p. 224)**
- **all** -- Set limits for all traffic.**(p. 207)**
- **ip** -- Apply the specified access control list to inbound packets on this INTERFACE list**(p. 225)**

receive

- interface vlan *VLAN-ID* ip rip receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:
- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

- interface vlan *VLAN-ID* ip rip *IP-ADDR* receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:
- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

- interface vlan *VLAN-ID* ip rip all receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:
- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

retransmit-interval

- interface vlan *VLAN-ID* ip ospf retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- interface vlan *VLAN-ID* ip ospf all retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

rip

- [no] interface vlan *VLAN-ID* ip rip

```
Usage: [no] ip rip [...]

Description: Enable/disable/configure Routing Internet Protocol (RIP)
             on the VLAN interface.
             Called without 'no', the command enables RIP on the interface.
             Otherwise ('no' is specified), the command disables RIP on the
             interface. The command can be followed by a RIP configuration
             command. Use 'ip rip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 212)**
- **authentication-key** -- Set RIP authentication key (maximum 16 characters).**(p. 211)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 235)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 248)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 258)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 260)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 260)**
- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 227)**
- **all** -- Process the request for all IP addresses.**(p. 207)**

rip-compatible

- interface vlan *VLAN-ID* ip rip *< V1-only | V2-only | V1-or-V2 >*

  ```
  Define RIP version for incoming and outgoing packets.
  ```

  Supported Values:

  - **V1-only** -- Use RIP version 1 only.
  - **V2-only** -- Use RIP version 2 only.
  - **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.
- interface vlan *VLAN-ID* ip rip *IP-ADDR < V1-only | V2-only | V1-or-V2 >*

  ```
  Define RIP version for incoming and outgoing packets.
  ```

  Supported Values:

  - **V1-only** -- Use RIP version 1 only.
  - **V2-only** -- Use RIP version 2 only.
  - **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.
- interface vlan *VLAN-ID* ip rip all *< V1-only | V2-only | V1-or-V2 >*

  ```
  Define RIP version for incoming and outgoing packets.
  ```

  Supported Values:

  - **V1-only** -- Use RIP version 1 only.
  - **V2-only** -- Use RIP version 2 only.
  - **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

send

- interface vlan *VLAN-ID* ip rip send *< disabled | V1-only | V1-compatible-V2 | ... >*

  ```
  Define RIP version for outgoing packets.
  ```

  Supported Values:

  - **disabled** -- Do not send RIP updates.
  - **V1-only** -- Send RIP version 1 updates only.
  - **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
  - **V2-only** -- Send RIP version 2 updates only.
- interface vlan *VLAN-ID* ip rip *IP-ADDR* send *< disabled | V1-only | V1-compatible-V2 | ... >*

  ```
  Define RIP version for outgoing packets.
  ```

  Supported Values:

- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

- interface vlan *VLAN-ID* ip rip all send *< disabled | V1-only | V1-compatible-V2 | ... >*

  ```
  Define RIP version for outgoing packets.
  ```

  Supported Values:
  - **disabled** -- Do not send RIP updates.
  - **V1-only** -- Send RIP version 1 updates only.
  - **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
  - **V2-only** -- Send RIP version 2 updates only.

speed-duplex

- interface *[ETHERNET] PORT-LIST* speed-duplex *< 10-half | 100-half | 10-full | ... >*

```
Usage: speed-duplex <10-half|100-half|10-full|100-full|1000-full|
                     auto|auto-10|auto-100|auto-1000|auto-10-100>

Description: Define mode of operation for the port(s).
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.

             For 10FL:
             - 10-half     10 Mbps, half duplex (default). The port operates
                           according to the IEEE 802.3/Ethernet standards.
             - 10-full     10 Mbps, full duplex. The port simultaneously
                           receives and transmits data. (The device attached
                           to the port must support full duplex operation).

             For 10/100TX:
                           Note: Make sure that the device attached to the
                           port is configured the same as the selection you
                           make here.
             - auto        (default) The port automatically selects the
                           network speed (10 or 100 Mbps), and that data
                           transfer operation (full or half duplex) between
                           the switch and another IEEE 802u-compliant device
                           running the 'Auto Negotiation' protocol.
             - 10-half     10 Mbps, half duplex.
             - 10-full     10 Mbps, full duplex.
             - 100-half    100 Mbps, half duplex.
             - 100-full    100 Mbps, full duplex.
             - auto-10     Same as 'auto' except that the port speed is fixed
                           at 10 Mbps. The data transfer operation (full or
                           half duplex) is auto negotiated.

             For 100FX:
             - 100-full    (default) 100 Mbps, full duplex.
             - 100-half    100 Mbps, half duplex.

             For 1000T:
             - auto        (default) The port automatically selects the
                           network speed (100 or 1000 Mbps)and the port
                           wiring operation (MDI-X or MDI) between the
                           switch and another IEEE 802.3ab-compliant device
```

```
                  running the 'Auto Negotiation' protocol.
- 100-full        100 Mbps, full duplex.
- auto-100        Same as 'auto'. Limited to 100Mbps network speed.
- auto-1000       Same as 'auto'. Limited to 1000Mbps network speed.
- auto-10-100     Same as 'auto'. Limited to 10Mbps or 100 Mbps
                  network speed.

For 1000SX, 1000LX:
- auto            (default) The port Auto Negotiates for Flow
                  Control if Flow Control is set to Enable.
- 1000-full       1000 Mbps, full duplex.

For 1000Stk:
- auto            Runs in 1000 Mbps, full duplex.
                  The port Auto Negotiates for Flow Control if
                  Flow Control is set to Enable.
```

Supported Values:

- **10-half** -- 10 Mbps, half duplex.
- **100-half** -- 100 Mbps, half duplex.
- **10-full** -- 10 Mbps, full duplex.
- **100-full** -- 100 Mbps, full duplex.
- **1000-full** -- 1000 Mbps, full duplex.
- **auto** -- Use Auto Negotiation for speed and duplex mode.
- **auto-10** -- 10 Mbps, use Auto Negotiation for duplex mode.
- **auto-100** -- 100 Mbps, use Auto Negotiation for duplex mode.
- **auto-1000** -- 1000 Mbps, use Auto Negotiation for duplex mode.
- **auto-10-100** -- 10 or 100 Mbps, and half or full duplex, using Auto Negotiation.

src-ip

- interface vlan *VLAN-ID* connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

- interface svlan *VLAN-ID* connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

svlan

- [no] interface svlan *VLAN-ID*

```
Usage: [no] svlan VLAN-ID [...]

Description: Add, delete, edit SVLAN configuration or enter a SVLAN context.
             If an existing 'SVLAN VLAN-ID' is specified you are put into the
             context for that SVLAN, and can then execute commands for that
             SVLAN. If a new VLAN-ID is specified, the new SVLAN is added with
             the VLAN-ID, and you are put into the context of the new SVLAN.
             If you follow the command with one of the SVLAN Context commands
             in the same command line, the context level is not changed, but
             the commands are executed for the SVLAN specified by the
             VLAN-ID. The 'no' option of the SVLAN command is used to delete
             the SVLAN specified by VLAN-ID.
```

Next Available Options:

- **dhcp-snooping** -- **(p. 217)**
- **ip** -- Configure various IP parameters for the VLAN**(p. 225)**

- **ipv6** -- Configure various IP parameters for the VLAN**(p. 230)**
- **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 212)**
- **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter**(p. 215)**
- **monitor** -- Define either the VLAN is to be monitored or not**(p. 238)**
- **name** -- Set the VLAN's name (ASCII-STR) **(p. 242)**
- **protocol** -- Set a predefined protocol for the current VLAN. **(p. 253)**
- **qos** -- Set VLAN-based priority**(p. 254)**
- **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 263)**
- **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 266)**
- **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 220)**
- **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network**(p. 267)**
- **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size**(p. 232)**

tagged

- [no] interface vlan *VLAN-ID* tagged *[ETHERNET] PORT-LIST*

```
Usage: [no] tagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as tagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- [no] interface svlan *VLAN-ID* tagged *[ETHERNET] PORT-LIST*

```
Usage: [no] tagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as tagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

timer-interval

- interface vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR* interval *< 1 to 255 >*

```
Timeout interval in seconds <1-255>.
```

Range: < 1 to 255 >

transit-delay

- interface vlan *VLAN-ID* ip ospf transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

- interface vlan *VLAN-ID* ip ospf *IP-ADDR* transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

- interface vlan *VLAN-ID* ip ospf all transit-delay *< 1 to 3600 >*

  ```
  Set transit delay in seconds; the default is 1.
  ```

  Range: < 1 to 3600 >

trust

- [no] interface *[ETHERNET] PORT-LIST* dhcp-snooping trust

  ```
  Usage: [no] dhcp-snooping trust PORT-LIST

  Description: Configure trusted interfaces. Only server packets received
               on trusted interfaces will be forwarded. When 'no' is
               specified the interfaces are marked as untrusted.
               The default port state is untrusted.

  Parameters:

      o PORT-LIST - Port list on which to configure trust status.
  ```

- [no] interface *[ETHERNET] PORT-LIST* arp-protect trust

ttl-threshold

- interface vlan *VLAN-ID* ip pim-dense ttl-threshold *< 0 to 255 >*

  ```
  Usage: ip pim-dense ttl-threshold <0-255>

  Description: Set the Time To Live in a PIM-DM State Refresh message at
               which it is not forwarded on this interface. Default is 0.
  ```

  Range: < 0 to 255 >

- interface vlan *VLAN-ID* ip mroute ttl-threshold *< 0 to 255 >*

  ```
  Usage: ip mroute ttl-threshold <0-255>

  Description: Set the multicast datagram TTL threshold for the interface.
               Any IP multicast datagrams with a TTL less than this threshold
               will not be forwarded out the interface. The default value of 0
               means all multicast packets are forwarded out the interface.
  ```

  Range: < 0 to 255 >

type

- interface *[ETHERNET] PORT-LIST* type *< Trunk | | | ... >*

  Supported Values:

  - **Trunk**
  -
  -
  - **10FL**
  - **10T**
  - **10/100TX**
  - **100FX**
  - **100FX-SFP**
  - **Vlan**
  - **Mesh**
  - **1000SX**

- **1000LX**
- **100/1000T**
- **1000T**
- **1000Stk**
- **1000LH**
- **10GbE-CX4**
- **10GbE-SR**
- **10GbE-ER**
- **10GbE-LR**
- **1000T-SFP**
- **1000X**

udp

- [no] interface vlan *VLAN-ID* ip forward-protocol udp

```
Usage: [no] ip forward-protocol udp IP-ADDR PORT-NUM|PORT-NAME

Description: Add or remove a UDP server address for the VLAN. The
             broadcast  packets received by the switch on this VLAN are to
             be forwarded to the specified application server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **ip-addr** -- IP address of the protocol server. (IP-ADDR) **(p. 227)**

unblock

- interface vlan *VLAN-ID* connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 207)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 224)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 262)**

- interface svlan *VLAN-ID* connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 207)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 224)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 262)**

unknown-vlans

- interface *[ETHERNET] PORT-LIST* unknown-vlans *< Learn | Block | Disable >*

```
Usage: unknown-vlans <learn|block|disable>

Description: Configure GVRP on the port(s).
```

```
               If 'learn' is specified then the port will accept join
               requests for new VLANs on this port and propagate a VLAN
               join requests through all other forwarding ports that are
               participating in GVRP.
               If 'block' is specified then the port will only process
               GRVP packets that concern themselves with known VLANs.
               If 'disable' is specified then all GRVP packets will be
               ignored.
               This is an Interface context command. It can be called directly
               from the interface context or follow the 'interface [ethernet]
               PORT-LIST' command.
```

Supported Values:

- **Learn** -- Learn new VLANs.
- **Block** -- Ignore new VLANs.
- **Disable** -- Ignore all GVRP packets.

untagged

- [no] interface vlan *VLAN-ID* untagged *[ETHERNET] PORT-LIST*

```
Usage: [no] untagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as untagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- [no] interface svlan *VLAN-ID* untagged *[ETHERNET] PORT-LIST*

```
Usage: [no] untagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as untagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

virtual-ip-address

- [no] interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* virtual-ip-address

```
Usage: [no] vrrp vrid <VRID> virtual-ip-address <IP-ADDR>

Description: Specify IP address to be supported by the virtual router instance.
             There is no default value.
```

Next Available Option:

- **ip-addr** -- Specify IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 227)**

vlan

- interface *[ETHERNET] PORT-LIST* link-keepalive vlan *VLAN-ID*

```
Set vlan-id for tagged UDLD control packets.
```

- [no] interface vlan *VLAN-ID*

```
Usage: [no] vlan VLAN-ID [...]
```

```
Description: Add, delete, edit VLAN configuration or enter a VLAN context.
             If an existing VLAN-ID is specified you are put into the
             context for that VLAN, and can then execute commands for that
             VLAN. If a new VLAN-ID is specified, the new VLAN is added with
             the VLAN-ID, and you are put into the context of the new VLAN.
             If you follow the command with one of the VLAN Context commands
             in the same command line, the context level is not changed, but
             the commands are executed for the VLAN specified by the
             VLAN-ID. The 'no' option of the VLAN command is used to delete
             the VLAN specified by VLAN-ID.
```

Next Available Options:

- **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 212)**
- **dhcp-snooping** -- **(p. 217)**
- **ip** -- Configure various IP parameters for the VLAN**(p. 225)**
- **igmp-proxy** -- Associate an IGMP proxy domain with a VLAN**(p. 224)**
- **ipv6** -- Configure various IP parameters for the VLAN**(p. 230)**
- **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter**(p. 215)**
- **monitor** -- Define either the VLAN is to be monitored or not**(p. 238)**
- **name** -- Set the VLAN's name (ASCII-STR) **(p. 242)**
- **protocol** -- Set a predefined protocol for the current VLAN. **(p. 253)**
- **qos** -- Set VLAN-based priority**(p. 254)**
- **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 263)**
- **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 266)**
- **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 220)**
- **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network**(p. 267)**
- **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size**(p. 232)**
- **vrrp** -- Enable/disable/configure VRRP operation on the VLAN**(p. 268)**
- **ip-recv-mac-address** -- Associates a L3-mac-address with a VLAN**(p. 229)**

voice

- [no] interface vlan *VLAN-ID* voice

```
Usage: [no] voice

Description: Labels this VLAN as a Voice VLAN, allowing you to separate,
             prioritize, and authenticate voice traffic moving through
             your network.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- [no] interface svlan *VLAN-ID* voice

```
Usage: [no] voice

Description: Labels this VLAN as a Voice VLAN, allowing you to separate,
             prioritize, and authenticate voice traffic moving through
             your network.
             This is a VLAN context command. It can be called directly
```

```
                from the VLAN context or follow the 'vlan VLAN-ID'
                command.
```

vrid

- [no] interface vlan *VLAN-ID* vrrp vrid *< 1 to 255 >*

```
Usage: [no] vrrp vrid <VRID> [...]

Description: Configure a virtual router instance for the VLAN.
             A virtual router is defined by its virtual router
             identifier (VRID) and a set of IP addresses for which
             virtual router acts as a Master or Backup. The scope
             of each virtual router is restricted to a single VLAN.
```

Range: < 1 to 255 >

Next Available Options:

- **backup** -- Designate the virtual router instance as a Backup**(p. 214)**
- **owner** -- Designate the virtual router instance as an Owner (Master)**(p. 244)**
- **virtual-ip-address** -- Specify IP address to be supported by the virtual router instance**(p. 266)**
- **primary-ip-address** -- Specify IP address the virtual router instance will use as a source in VRRP advertisement messages**(p. 251)**
- **advertise-interval** < 1 to 255 > -- Set time interval (in seconds) between sending VRRP advertisement messages**(p. 206)**
- **priority** < 1 to 255 > -- Configure priority for the virtual router instance**(p. 251)**
- **preempt-mode** -- Enable/disable preempt mode for the virtual router instance**(p. 250)**
- **preempt-delay-time** < 1 to 600 > -- Enable the pre-emptive delay timer for the virtual router instance**(p. 250)**
- **enable** -- Enable/disable operation of the virtual router instance**(p. 219)**

vrrp

- [no] interface vlan *VLAN-ID* vrrp

```
Usage: [no] vlan <VLAN-ID> vrrp vrid <VRID> [...]

Description: Enable/disable/configure VRRP operation on the VLAN.
             Use 'vrrp vrid <VRID> ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly from
             the VLAN context or follow the 'vlan VLAN-ID' command.
```

Next Available Option:

- **vrid** < 1 to 255 > -- Configure a virtual router instance for the VLAN**(p. 268)**

ip

OVERVIEW

Category:	
Primary context:	config
Related Commands	**ipv6 (page 291)** **show ip (page 480)**

```
Usage: [no] ip ...

Description: Configure various IP parameters for the switch. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
```

COMMAND STRUCTURE

- [no] ip **access-list** -- Enter the named-acl context for the specified access control list **(p. 272)**
  - **connection-rate-filter** -- Configure a connection-rate-filter Access Control List. **(p. 275)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**
  - **extended** -- Configure an extended Access Control List. **(p. 277)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**
    - **number < 100 to 199 >** -- Specify Access Control List to configure by number. **(p. 283)**
  - **resequence** -- Renumber the entries in an Access Control List. **(p. 284)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**
      - **start-seq-num < 1 to 2147483647 >** -- Specify the starting sequence number. **(p. 288)**
        - **increment < 1 to 2147483646 >** -- Specify the increment. **(p. 279)**
  - **standard** -- Configure a standard Access Control List. **(p. 288)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**
    - **number < 1 to 99 >** -- Specify Access Control List to configure by number. **(p. 283)**
- [no] ip **address** -- Set IP parameters for communication within an IP network **(p. 272)**
  - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 276)**
  - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 280)**
- [no] ip **arp-age** -- Modify Address Resolution Protocol (ARP) table entry timeout, specified in minutes **(p. 273)**
  - **infinite** -- Causes the ARP timeout to be set to 0, indicating an infinite timeout period. **(p. 279)**
  - **timeout < 1 to 1440 >** -- Modify Address Resolution Protocol (ARP) table entry timeout, specified in minutes (NUMBER) **(p. 288)**
- [no] ip **authorized-managers** -- Define the IPV4 addresses allowed to manage the switch **(p. 273)**
  - **IPV4-ADDR** -- Authorized manager IPv4 address. (IP-ADDR) **(p. 281)**
    - **access < Manager | Operator >** -- Define an access level desired. **(p. 272)**
    - **IPV4-MASK** -- IP mask defining a group of adjacent manager IP addresses. (IP-ADDR) **(p. 281)**
- [no] ip **default-gateway** -- Configure the IPv4 default gateway address, which will be used when routing is not enabled on the switch **(p. 275)**
  - **ipaddr** -- IPv4 address of the default gateway. (IP-ADDR) **(p. 280)**
- [no] ip **directed-broadcast** -- Enable/disable directed broadcast forwarding **(p. 276)**
- [no] ip **dns** -- Configure the DNS (Domain Name System) default domain suffix and the name server IP address for translation of hostnames to IP addresses **(p. 276)**
  - **domain-name** -- Configure default domain suffix. **(p. 277)**
    - **domain-name** -- Default domain suffix. (ASCII-STR) **(p. 277)**
  - **server-address** -- Configure DNS server IP address. **(p. 286)**

    - **priority < 1 to 3 >** -- Priority of Server Address. (NUMBER) **(p. 283)**
      - **ip6addr** -- DNS server IPv6 address. (IPV6-ADDR) **(p. 280)**
      - **ipaddr** -- DNS server IP address. (IP-ADDR) **(p. 280)**
- [no] ip **icmp** -- Configure ICMP Rate Limiting capacity **(p. 278)**
  - **addrmask** -- Enable/disable address mask replies **(p. 273)**
  - **burst-normal < 0 to 1000000 >** -- The maximum number of icmp replies to send per second **(p. 275)**
  - **echo** -- Enable/disable echo replies to broadcast echo requests **(p. 277)**
    - **broadcast-request < Min | Max >** -- Enable/disable echo replies to broadcast echo requests **(p. 274)**
  - **redirects** -- Enable/disable redirect error messages **(p. 284)**
  - **reply-limit** -- Enable/disable ICMP reply rate limiting **(p. 284)**
  - **unreachable** -- Enable/disable destination unreachable error messages **(p. 289)**
- [no] ip **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature **(p. 278)**
  - **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 274)**
  - **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 274)**
  - **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 277)**
  - **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 278)**
  - **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 278)**
  - **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups **(p. 278)**
  - **querier** -- Specify querier/non-querier capability for the VLAN **(p. 284)**
    - **interval < 5 to 300 >** -- Sets the interval in seconds between IGMP queries (default: 125) **(p. 279)**
- [no] ip **irdp** -- Enable/disable ICMP Router Discovery Protocol (IRDP) **(p. 281)**
- [no] ip **load-sharing** -- Specify the maximum number of equal cost IP load sharing paths **(p. 281)**
  - **load-sharing-value < 2 to 4 >** -- Specify the maximum number of equal cost IP load sharing paths **(p. 282)**
- [no] ip **multicast-routing** -- Enable/disable IP multicast routing on the device **(p. 282)**
- ip **preserve** -- **(p. 283)**
- [no] ip **route** -- Add or delete static routing table entries **(p. 285)**
  - **ip-addr** -- Specify IP address and mask of the route destination. (IP-ADDR/MASK-LENGTH) **(p. 280)**
    - **blackhole** -- Specify that packets are silently discarded with no ICMP message sent. **(p. 274)**
      - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 276)**
    - **ip-addr** -- Specify gateway IP address. (IP-ADDR) **(p. 280)**
      - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 276)**
    - **reject** -- Specify that packets are discarded and ICMP error is returned to sender. **(p. 284)**
      - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 276)**
    - **vlan** -- Specify the destination VLAN. (VLAN-ID) **(p. 289)**
      - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 276)**
- [no] ip **router-id** -- Define the device router id **(p. 285)**
  - **ipaddr** -- Define the device router id (IP-ADDR) **(p. 280)**
- [no] ip **routing** -- Enable/disable IP routing support on the device **(p. 286)**

- [no] ip **source-binding** -- Add/remove a static IP-to-MAC binding in the DHCP snooping database **(p. 286)**
  - **vlan** -- (VLAN-ID) **(p. 289)**
    - **ip** -- (IP-ADDR) **(p. 280)**
      - **mac** -- (MAC-ADDR) **(p. 282)**
        - **interface** -- ([ethernet] PORT-NUM) **(p. 279)**
- [no] ip **source-route** -- Enable/disable forwarding of source routed packets **(p. 287)**
- [no] ip **ssh** -- Enable/disable SSH server on the device or set various SSH server parameters **(p. 287)**
  - **filetransfer** -- Enable/disable secure file transfer capability. **(p. 277)**
  - **ip-version < 4 | 6 | 4or6 >** -- Specify the type of connections the daemon should listen for. **(p. 281)**
  - **port** -- Specify the TCP port on which the daemon should listen for SSH connections. **(p. 283)**
    - **default** -- Specify that the daemon should listen on the default TCP port (22). **(p. 275)**
    - **IP-PORT** -- Specify the TCP port number on which the daemon should listen. (TCP/UDP-PORT) **(p. 281)**
  - **public-key < manager | operator >** -- Configure a client public-key. (NUMBER) **(p. 283)**
    - **keystring** -- ASCII formatted public-key. (ASCII-STR) **(p. 281)**
  - **timeout < 5 to 120 >** -- Specify the maximum length of time (seconds) permitted for protocol negotiation and authentication. (NUMBER) **(p. 288)**
- [no] ip **timep** -- Configure the method to acquire the Timep server address **(p. 288)**
  - **dhcp** -- Use DHCP to acquire Timep server address. **(p. 275)**
    - **interval < 1 to 9999 >** -- Specify how often (in minutes) the switch tries to get the current time. **(p. 279)**
  - **manual** -- Manually configure the Timep server address. **(p. 282)**
    - **server** -- Timep server IPv4 address. (IP-ADDR) **(p. 286)**
      - **interval < 1 to 9999 >** -- Specify how often (in minutes) the switch tries to get the current time. **(p. 279)**
    - **serverV6** -- Timep server IPv6 address. (IPV6-ADDR) **(p. 286)**
      - **interval < 1 to 9999 >** -- Specify how often (in minutes) the switch tries to get the current time. **(p. 279)**
- ip **ttl < 2 to 255 >** -- Specify TTL for outgoing IP packets (NUMBER) **(p. 289)**
- [no] ip **udp-bcast-forward** -- Enable/disable UDP broadcast forwarding **(p. 289)**
- [no] ip **zero-broadcast** -- Enable/disable usage of zero broadcast IP Address **(p. 290)**

COMMAND DETAILS

access

- ip authorized-managers *IP-ADDR* access < *Manager* | *Operator* >

```
Define an access level desired.
```

Supported Values:

- **Manager**
- **Operator**

access-list

- [no] ip access-list

```
Usage: [no] ip access-list <extended|standard|conection-rate-filter> <ACL-ID>

Description: Enter the named-acl context for the specified access control
             list.  The ACL-ID is case sensitive and may be up to sixty-four
             characters in length.  If it includes spaces, the entire ACL-ID
             must be enclosed in quotation marks.
```

Next Available Options:

- **extended** -- Configure an extended Access Control List. **(p. 277)**
- **standard** -- Configure a standard Access Control List. **(p. 288)**
- **resequence** -- Renumber the entries in an Access Control List. **(p. 284)**
- **connection-rate-filter** -- Configure a connection-rate-filter Access Control List. **(p. 275)**

address

- [no] ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.

Parameters:

    o dhcp-bootp - The switch attempts to get its configuration from a
      DHCP/Bootp server.

    o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch.
      The IP-ADDR/MASK-LENGTH may be specified in two ways using the
      following syntax:
          ip address 192.32.36.87/24
          ip address 192.32.36.87 255.255.255.0
      Both of the statements above would have the same effect.
```

Next Available Options:

- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 280)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 276)**

addrmask

- [no] ip icmp addrmask

```
Usage: [no] ip icmp addrmask

Description: Enable/disable address mask replies.
```

arp-age

- [no] ip arp-age

```
Usage: [no] ip arp-age <[0..1440]|infinite>

Description: Modify Address Resolution Protocol (ARP) table entry timeout,
             specified in minutes. You can set the age up to 1440 minutes (24 hours).

              The default timeout is 20 minutes.

     o   <0..1440> - timeout specified in minutes.

     o   infinite - sets the timeout to 0. A value of 0 indicates an infinite
         timeout to the switch. (Internally the ARP age timeout is set to 99,999,999

         seconds (approximately 3.2 years)
```

Next Available Options:

- **timeout** < 1 to 1440 > -- Modify Address Resolution Protocol (ARP) table entry timeout, specified in minutes (NUMBER) **(p. 288)**
- **infinite** -- Causes the ARP timeout to be set to 0, indicating an infinite timeout period. **(p. 279)**

Example 1. Example of ip arp-age Command

ProCurve(config)# ip arp-age 1000

authorized-managers

- [no] ip authorized-managers

```
Usage: [no] ip authorized-managers <IPV4-ADDR [IPV4-MASK]>
               access [manager|operator] [IPV4-MASK]

Description: Define the IPV4 addresses allowed to manage the switch.
             Clients using the specified IPV4 addresses are allowed
             to access the switch's web browser interface, telnet to
             the switch and to perform TFTP operations.
             A maximum of 10 addresses may be configured.

Parameters:

    o IPV4-ADDR - The IPV4 address of an authorized manager.

    o IPV4-MASK - A mask that allows you to define which portions of
```

```
          the listed IP address need to be matched by an incoming request.
          The default mask is 255.255.255.255. For example, with an
          authorized address of 10.8.11.1 and a mask of 255.255.255.255,
          only access from 10.8.11.1 is allowed. With a mask of
          255.255.255.0, access from any IP address with 10.8.11.x is
          allowed.

        o [manager|operator] - A designation of the management capabilities
          that are accessible to the authorized manager.
          'manager' allows full access to all web browser and telnet to console
          for viewing and setting the switch configuration, and for performing
          all other interface operations,including all TFTP operations.
          'operator' allows view-only access from the web browser and the
          console, but does not allow changing the switch configuration or any
          TFTP operations. The default access level is manager.
```

Next Available Option:

- **IPV4-ADDR** -- Authorized manager IPv4 address. (IP-ADDR) **(p. 281)**

auto

- ip igmp auto *[ETHERNET] PORT-LIST*

```
Usage: ip igmp auto [ethernet] PORT-LIST

Description: Instruct the device to monitor incoming multicast traffic
             on the specified ports (this is the default behavior).  This
             feature is configured on a per-VLAN basis.
```

blackhole

- [no] ip route *IP-ADDR/MASK-LENGTH* blackhole

```
Specify that packets are silently discarded with no ICMP message sent.
```

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 276)**

blocked

- ip igmp blocked *[ETHERNET] PORT-LIST*

```
Usage: ip igmp blocked [ethernet] PORT-LIST

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

broadcast-request

- [no] ip icmp echo broadcast-request

```
Usage: [no] ip icmp echo broadcast-request

Description: Enable/disable echo replies to broadcast echo requests.
```

Supported Values:
- **Min**
- **Max**

burst-normal

- [no] ip icmp burst-normal *< 0 to 1000000 >*

```
Usage: ip icmp burst-normal <0-1000000>

Description: The maximum number of icmp replies to send per second.
             The default value is 1000.
```

Range: < 0 to 1000000 >

connection-rate-filter

- [no] ip access-list connection-rate-filter

```
Configure a connection-rate-filter Access Control List.
```

Next Available Option:
- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**

default

- ip ssh port default

```
Specify that the daemon should listen on the default TCP port (22).
```

default-gateway

- [no] ip default-gateway

```
Usage: [no] ip default-gateway [IP-ADDR]

Description: Configure the IPv4 default gateway address, which will be
             used when routing is not enabled on the switch. The IP-ADDR
             must be specified if the command is not preceded by 'no'.
             Preceding the command with 'no' deletes the default gateway
             address.
```

Next Available Option:
- **ipaddr** -- IPv4 address of the default gateway. (IP-ADDR) **(p. 280)**

dhcp

- ip timep dhcp

```
Use DHCP to acquire Timep server address.
```

Next Available Option:
- **interval** < 1 to 9999 > -- Specify how often (in minutes) the switch tries to get the current time.**(p. 279)**

dhcp-bootp

- ip address dhcp-bootp

```
Configure the interface to use DHCP/Bootp server to acquire parameters.
```

directed-broadcast

- [no] ip directed-broadcast

```
Usage: [no] ip directed-broadcast

Description: Enable/disable directed broadcast forwarding.
```

distance

- ip route *IP-ADDR/MASK-LENGTH IP-ADDR* distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

- ip route *IP-ADDR/MASK-LENGTH* vlan *VLAN-ID* distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

- ip route *IP-ADDR/MASK-LENGTH* reject distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

- ip route *IP-ADDR/MASK-LENGTH* blackhole distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

dns

- [no] ip dns

```
Usage: [no] ip dns domain-name <domain-name>
       [no] ip dns server-address priority <PRIORITY> [IP-ADDR|IPV6-ADDR]

Description: Configure the DNS (Domain Name System) default domain suffix
             and the name server IP address for translation of hostnames
             to IP addresses.
             No additional parameters are required when 'no' is specified.

Parameters:
    o domain-name <domain-name> - The default domain suffix.
    o server-address priority <PRIORITY> [IP-ADDR|IPV6-ADDR]
      <PRIORITY> priority of the domain name server address.
      [IP-ADDR|IPV6-ADDR] IPv4 or IPv6 address.
```

Next Available Options:

- **domain-name** -- Configure default domain suffix.**(p. 277)**
- **server-address** -- Configure DNS server IP address.**(p. 286)**

domain-name

- [no] ip dns domain-name

  ```
  Configure default domain suffix.
  ```

  Next Available Option:

  - **domain-name** -- Default domain suffix. (ASCII-STR) **(p. 277)**

- ip dns domain-name *DOMAIN-NAME*

  ```
  Default domain suffix.
  ```

echo

- [no] ip icmp echo

  ```
  Usage: [no] ip icmp echo ...

  Description: Enable/disable echo replies to broadcast echo requests.
  ```

  Next Available Option:

  - **broadcast-request** < Min | Max > -- Enable/disable echo replies to broadcast echo requests**(p. 274)**

extended

- [no] ip access-list extended

  ```
  Configure an extended Access Control List.
  ```

  Next Available Options:

  - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**
  - **number** < 100 to 199 > -- Specify Access Control List to configure by number. **(p. 283)**

fastleave

- [no] ip igmp fastleave *[ETHERNET] PORT-LIST*

  ```
  Usage: [no] ip igmp fastleave [ethernet] PORT-LIST

  Description: Enables or disables IGMP Fast Leaves. When enabled, as soon as
               an IGMP Group Leave has been received on a non-cascaded port,
               the switch stops forwarding multicast traffic for that group
               to that port.
               Does not apply to cascaded ports (see ip igmp forcedfastleave).
               When disabled, or when the port is cascaded, the regular IGMP
               leave time is used (up to 10 seconds when the switch is not
               the IGMP Querier).
               The default behavior is for IGMP FastLeaves to be enabled.
               This feature is configured for ports on a per-VLAN basis.
  ```

filetransfer

- [no] ip ssh filetransfer

  ```
  Enable/disable secure file transfer capability.
  ```

forcedfastleave

- [no] ip igmp forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forcedfastleave [ethernet] PORT-LIST

Description: When enabled, this feature forces IGMP Fast Leaves to occur
             even when the port is cascaded. See 'ip igmp fastleave' for
             more information.  The default behavior is for IGMP Forced
             FastLeaves to be disabled.
             This feature is configured for ports on a per-VLAN basis.
```

forward

- ip igmp forward *[ETHERNET] PORT-LIST*

```
Usage: ip igmp forward [ethernet] PORT-LIST

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

high-priority-forward

- [no] ip igmp high-priority-forward

```
Usage: [no] ip igmp high-priority-forward

Description: Enable/disable the high priority forwarding of traffic for
             subscribed IP Multicast groups. This feature is configured on
             a per-VLAN  basis.
```

icmp

- [no] ip icmp

```
Usage: [no] ip icmp [...]

Description: Configure ICMP Rate Limiting capacity. Use 'ip icmp ?' to get
             a list of all possible configurable parameters.
```

Next Available Options:

- **addrmask** -- Enable/disable address mask replies**(p. 273)**
- **burst-normal** < 0 to 1000000 > -- The maximum number of icmp replies to send per second**(p. 275)**
- **echo** -- Enable/disable echo replies to broadcast echo requests**(p. 277)**
- **redirects** -- Enable/disable redirect error messages**(p. 284)**
- **reply-limit** -- Enable/disable ICMP reply rate limiting**(p. 284)**
- **unreachable** -- Enable/disable destination unreachable error messages**(p. 289)**

igmp

- [no] ip igmp

```
Usage: [no] ip igmp [...]

Description: Enable/disable/configure IP Multicast Group Protocol (IGMP)
             feature.  This command enables, disables or configures the
```

```
IGMP feature for IGMP communication between Multicast
Routers, Multicast Servers, and Multicast Clients connected
to the switch.  If not preceded by 'no', the command accepts
a variety of configuration parameters. To get a list of all
available parameters use 'ip igmp ?'. To get a detailed help
for a parameter, follow it with 'help' keyword.
```

Next Available Options:

- **querier** -- Specify querier/non-querier capability for the VLAN**(p. 284)**
- **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups**(p. 278)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 274)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 274)**
- **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 277)**
- **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 278)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 278)**

increment

- ip access-list resequence *NAME < 1 to 2147483647 > < 1 to 2147483646 >*

```
Specify the increment.
```

Range: < 1 to 2147483646 >

infinite

- ip arp-age infinite

```
Causes the ARP timeout to be set to 0, indicating an infinite
 timeout period.
```

interface

- ip source-binding *VLAN-ID IP-ADDR MAC-ADDR [ETHERNET] PORT-NUM*

```
See ip source-binding command.
```

interval

- ip igmp querier interval *< 5 to 300 >*

```
Sets the interval in seconds between IGMP queries
 (default: 125)
```

Range: < 5 to 300 >

- ip timep dhcp interval *< 1 to 9999 >*

```
Specify how often (in minutes) the switch tries to get the current time.
```

Range: < 1 to 9999 >

- ip timep manual *IP-ADDR* interval *< 1 to 9999 >*

```
Specify how often (in minutes) the switch tries to get the current time.
```

Range: < 1 to 9999 >

- ip timep manual *IPV6-ADDR* interval *< 1 to 9999 >*

```
Specify how often (in minutes) the switch tries to get the current time.
```

Range: < 1 to 9999 >

ip

- ip source-binding *VLAN-ID IP-ADDR*

Next Available Option:

- **mac** -- (MAC-ADDR) **(p. 282)**

ip6addr

- [no] ip dns server-address priority *< 1 to 3 > IPV6-ADDR*

```
DNS server IPv6 address.
```

ipaddr

- ip default-gateway *IP-ADDR*

```
IPv4 address of the default gateway.
```

- [no] ip dns server-address priority *< 1 to 3 > IP-ADDR*

```
DNS server IP address.
```

- ip router-id *IP-ADDR*

```
Usage: ip router-id IP-ADDR
       [no] ip router-id

Description: Define the device router id.
             The no form of the command clears the router-id.
```

ip-addr

- [no] ip address *IP-ADDR/MASK-LENGTH*

```
Interface IP address/mask.
```

- ip route *IP-ADDR/MASK-LENGTH*

```
Specify IP address and mask of the route destination.
```

Next Available Options:

- **ip-addr** -- Specify gateway IP address. (IP-ADDR) **(p. 280)**
- **vlan** -- Specify the destination VLAN. (VLAN-ID) **(p. 289)**
- **reject** -- Specify that packets are discarded and ICMP error is returned to sender.**(p. 284)**
- **blackhole** -- Specify that packets are silently discarded with no ICMP message sent.**(p. 274)**

- [no] ip route *IP-ADDR/MASK-LENGTH IP-ADDR*

```
Specify gateway IP address.
```

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 276)**

IP-PORT

- ip ssh port *TCP/UDP-PORT*

```
Specify the TCP port number on which the daemon should listen.
```

IPV4-ADDR

- ip authorized-managers *IP-ADDR*

```
Authorized manager IPv4 address.
```

Next Available Options:

- **IPV4-MASK** -- IP mask defining a group of adjacent manager IP addresses. (IP-ADDR) **(p. 281)**
- **access** < Manager | Operator > -- Define an access level desired.**(p. 272)**

IPV4-MASK

- ip authorized-managers *IP-ADDR IP-ADDR*

```
IP mask defining a group of adjacent manager IP addresses.
```

ip-version

- ip ssh ip-version *< 4 | 6 | 4or6 >*

```
Specify the type of connections the daemon should listen for.
```

Supported Values:

- **4** -- Accept IPv4 connections only.
- **6** -- Accept IPv6 connections only.
- **4or6** -- Accept both IPv4 and IPv6 connections.

irdp

- [no] ip irdp

```
Usage: [no] ip irdp

Description: Enable/disable ICMP Router Discovery Protocol (IRDP).
             To configure IRDP, execute '[no] ip irdp [...]' from the
             VLAN context for the VLAN on which you wish to configure IRDP.
```

keystring

- ip ssh public-key *< manager | operator > KEYSTRING*

```
ASCII formatted public-key.
```

load-sharing

- [no] ip load-sharing

```
Usage: ip load-sharing <2-4>
       no ip load-sharing

Description: Specify the maximum number of equal cost IP load sharing
             paths.  no ip load-sharing disables IP load sharing.
```

Next Available Option:

- **load-sharing-value** < 2 to 4 > -- Specify the maximum number of equal cost IP load sharing paths**(p. 282)**

load-sharing-value

- ip load-sharing *< 2 to 4 >*

```
Usage: ip load-sharing <2-4>
       no ip load-sharing

Description: Specify the maximum number of equal cost IP load sharing
             paths.  no ip load-sharing disables IP load sharing.
```

Range: < 2 to 4 >

mac

- ip source-binding *VLAN-ID IP-ADDR MAC-ADDR*

Next Available Option:

- **interface** -- ([ethernet] PORT-NUM) **(p. 279)**

manual

- ip timep manual

```
Manually configure the Timep server address.
```

Next Available Options:

- **server** -- Timep server IPv4 address. (IP-ADDR) **(p. 286)**
- **serverV6** -- Timep server IPv6 address. (IPV6-ADDR) **(p. 286)**

multicast-routing

- [no] ip multicast-routing

```
Usage: [no] ip multicast-routing

Description: Enable/disable IP multicast routing on the device.
```

name

- [no] ip access-list extended *NAME*

```
Specify name of Access Control List to configure.
```

- [no] ip access-list standard *NAME*

```
Specify name of Access Control List to configure.
```

- ip access-list resequence *NAME*

  ```
  Specify name of Access Control List to configure.
  ```

  Next Available Option:
  - **start-seq-num** < 1 to 2147483647 > -- Specify the starting sequence number. **(p. 288)**

- [no] ip access-list connection-rate-filter *NAME*

  ```
  Specify name of Access Control List to configure.
  ```

number

- [no] ip access-list extended *< 100 to 199 >*

  ```
  Specify Access Control List to configure by number.
  ```

  Range: < 100 to 199 >
- [no] ip access-list standard *< 1 to 99 >*

  ```
  Specify Access Control List to configure by number.
  ```

  Range: < 1 to 99 >

port

- ip ssh port

  ```
  Specify the TCP port on which the daemon should listen for SSH connections.
  ```

  Next Available Options:
  - **IP-PORT** -- Specify the TCP port number on which the daemon should listen. (TCP/UDP-PORT) **(p. 281)**
  - **default** -- Specify that the daemon should listen on the default TCP port (22).**(p. 275)**

preserve

- ip preserve

priority

- [no] ip dns server-address priority *< 1 to 3 >*

  ```
  Priority of Server Address.
  ```

  Range: < 1 to 3 >

  Next Available Options:
  - **ipaddr** -- DNS server IP address. (IP-ADDR) **(p. 280)**
  - **ip6addr** -- DNS server IPv6 address. (IPV6-ADDR) **(p. 280)**

public-key

- ip ssh public-key *< manager | operator >*

  ```
  Configure a client public-key.
  ```

Supported Values:

- **manager** -- Select manager public keys.
- **operator** -- Select operator public keys.

Next Available Option:

- **keystring** -- ASCII formatted public-key. (ASCII-STR) **(p. 281)**

querier

- [no] ip igmp querier

```
Usage: [no] ip igmp querier [interval <seconds>]

Description: Specify querier/non-querier capability for the VLAN. IGMP
             queries are not sent when the mode is disabled. When
             enabled, the device cannot become Querier for the subnet
             unless the VLAN has an IP Address (use the 'show ip' command
             to determine this).  Each subnet must have at least one IGMP
             Querier-capable device in order for IGMP to function
             properly.  The querier interval setting modifies the time (in
             seconds) between IGMP queries.
```

Next Available Option:

- **interval** < 5 to 300 > -- Sets the interval in seconds between IGMP queries (default: 125) **(p. 279)**

redirects

- [no] ip icmp redirects

```
Usage: [no] ip icmp redirects

Description: Enable/disable redirect error messages.
```

reject

- [no] ip route *IP-ADDR/MASK-LENGTH* reject

```
Specify that packets are discarded and ICMP error is returned to sender.
```

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 276)**

reply-limit

- [no] ip icmp reply-limit

```
Usage: ip icmp reply-limit

Description: Enable/disable ICMP reply rate limiting.
```

resequence

- ip access-list resequence

```
Renumber the entries in an Access Control List.
```

Next Available Option:

- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**

route

- [no] ip route

```
Usage: [no] ip route IP-ADDR/MASK-LENGTH
             <IP-ADDR|vlan <vlan-id>|reject|blackhole> [distance <1-255>]

Description: Add or delete static routing table entries. A route
             entry is identified by a destination (IP-ADDR/MASK-LENGTH)
             and next-hop pair. The next-hop can be either a gateway IP
             address or a vlan or the keyword 'reject' or 'blackhole':
             - a gateway IP address indicates that the specified gateway
               will be used to reach the destination. The gateway address is
               not required to be directly reachable on one of local subnets.
               If the gateway address is not directly reachable, the route
               will be added to the routing table as soon as a route to the
               gateway address is learned.
               If the gateway address is one of local interface addresses,
               the destination is treated as if it is directly connected to
               the specified interface.
             - the keyword 'vlan' followed by the vlan-id indicates the
               destination vlan for that route.
             - the keyword 'reject' indicates that if this route is matched,
               a packet to the destination is discarded and a notification
               (e.g. ICMP error) is returned to the packet sender.
             - the keyword 'blackhole' indicates that if this route is matched,
               a packet to the destination is silently discarded and no
               notification (e.g. ICMP error) is returned to the packet sender.
             - the optional keyword 'distance' is used to specify the
               administrative distance for the route.
             If the route command is preceded by 'no' the command deletes
             the route for the specified destination next-hop pair.
```

Next Available Option:

- **ip-addr** -- Specify IP address and mask of the route destination. (IP-ADDR/MASK-LENGTH) **(p. 280)**

router-id

- [no] ip router-id

```
Usage: ip router-id IP-ADDR
       [no] ip router-id

Description: Define the device router id.
             The no form of the command clears the router-id.
```

Next Available Option:

- **ipaddr** -- Define the device router id (IP-ADDR) **(p. 280)**

routing

- [no] ip routing

```
Usage: [no] ip routing

Description: Enable/disable IP routing support on the device.
```

server

- ip timep manual *IP-ADDR*

```
Timep server IPv4 address.
```

Next Available Option:

- **interval** < 1 to 9999 > -- Specify how often (in minutes) the switch tries to get the current time.**(p. 279)**

server-address

- [no] ip dns server-address

```
Configure DNS server IP address.
```

Next Available Option:

- **priority** < 1 to 3 > -- Priority of Server Address. (NUMBER) **(p. 283)**

serverV6

- ip timep manual *IPV6-ADDR*

```
Timep server IPv6 address.
```

Next Available Option:

- **interval** < 1 to 9999 > -- Specify how often (in minutes) the switch tries to get the current time.**(p. 279)**

source-binding

- [no] ip source-binding

```
Usage: [no] ip source-binding <VLAN-ID> <MAC-ADDR> <IP-ADDR>
                             [ethernet] <PORT-NUM>

Description: Add/remove a static IP-to-MAC binding in the DHCP snooping
             database.

Parameters:
  o <VLAN-ID>   -- VLAN ID number to bind with the specified IP and MAC
                   address on the specified port in the DHCP snooping
                   binding database.
  o <MAC-ADDR>  -- MAC address to bind with the specified IP address and
                   VLAN on the specified port.
  o <IP-ADDR>   -- IP address to bind with the specified MAC address and
                   VLAN on the specified port.
```

```
o [ethernet] <PORT-NUM> -- Port number on which the IP-to-MAC and VLAN
                           binding is configured in.
```

Next Available Option:

- **vlan** -- (VLAN-ID) **(p. 289)**

source-route

- [no] ip source-route

```
Usage: [no] ip source-route

Description: Enable/disable forwarding of source routed packets.
```

ssh

- [no] ip ssh

```
Usage: ip ssh filetransfer
              port <<1-65535>|default>
              public-key <operator|manager> KEYSTRING
              ip-version <4|6|4or6>
              timeout <5-120>
       no ip ssh [filetransfer]

Description: Enable/disable SSH server on the device or set various SSH
             server parameters.

Parameters:

           o 'filetransfer' - Enable/disable secure file transfer
             capability.  (SCP and SFTP) Secure file transfer will not
             function unless SSH is also enabled.

           o 'port <<1-65535>|default>' - Set the TCP port on which the
             daemon should listen for SSH connections. The default is 22.

           o 'public-key <operator|manager> KEYSTRING' - set a key for
             public-key authentication.  The KEYSTRING parameter must be
             enclosed in quotes--either"KEYSTRING" or 'KEYSTRING'.
             Newlines may be escaped with a backslash.

           o 'ip-version <4|6|4or6>' - Select the IP mode to run in.
             'ip-version 4' will only accept connections from IPv4
             clients. 'ip-version 6' will only accept connections from
             IPv6 clients. 'ip-version 4or6' accept connections from
             both IPv4 and IPv6 clients. default is 'ip-version 4or6'.

           o 'timeout <5-120>' - Set the maximum length of time in
             seconds permitted for initial protocol negotiation and
             authentication. The default is 120 seconds.
```

Next Available Options:

- **filetransfer** -- Enable/disable secure file transfer capability.**(p. 277)**
- **port** -- Specify the TCP port on which the daemon should listen for SSH connections.**(p. 283)**
- **public-key** < manager | operator > -- Configure a client public-key. (NUMBER) **(p. 283)**

- **timeout** < 5 to 120 > -- Specify the maximum length of time (seconds) permitted for protocol negotiation and authentication. (NUMBER) **(p. 288)**
- **ip-version** < 4 | 6 | 4or6 > -- Specify the type of connections the daemon should listen for.**(p. 281)**

standard

- [no] ip access-list standard

```
Configure a standard Access Control List.
```

Next Available Options:

- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 282)**
- **number** < 1 to 99 > -- Specify Access Control List to configure by number. **(p. 283)**

start-seq-num

- ip access-list resequence *NAME < 1 to 2147483647 >*

```
Specify the starting sequence number.
```

Range: < 1 to 2147483647 >

Next Available Option:

- **increment** < 1 to 2147483646 > -- Specify the increment. **(p. 279)**

timeout

- ip arp-age *< 1 to 1440 >*

```
Usage: [no] ip arp-age <[0..1440]|infinite>

Description: Modify Address Resolution Protocol (ARP) table entry timeout,
             specified in minutes.
             The default timeout is 20 minutes.

      o   <0..1440> - timeout specified in minutes.

      o   infinite - sets the timeout to 0. A value of 0 indicates an infinite
          timeout to the switch.
```

Range: < 1 to 1440 >

- ip ssh timeout *< 5 to 120 >*

```
Specify the maximum length of time (seconds) permitted for protocol negotiation and
authentication.
```

Range: < 5 to 120 >

timep

- [no] ip timep

```
Usage: [no] ip timep [<dhcp|[manual <IP-ADDR | IPV6-ADDR>]> [interval <1-9999>]]

Description: Configure the method to acquire the Timep server address.
```

```
                No additional parameters are required when 'no' is specified.

Parameters:

    o <dhcp|manual> - The method the switch uses to acquire
      the Timep server address: dhcp - from a DHCP server; manual - you
      manually enter the Timep server address; disable (which is set by
      specifying the 'no' parameter) - the switch will not attempt to get
      its time from a Timep server.

    o [interval <1-9999>] (default is 720) How often (in minutes) the
      switch tries to get the current time.

    o [server <IP-ADDR>] - The IPv4 address of the Timep server that the
      switch gets the current time from.
    o [server <IPV6-ADDR>] - The IPv6 address of the Timep server that the
      switch gets the current time from.
```

Next Available Options:

- **dhcp** -- Use DHCP to acquire Timep server address.**(p. 275)**
- **manual** -- Manually configure the Timep server address.**(p. 282)**

ttl

- ip ttl *< 2 to 255 >*

```
Usage: ip ttl <2-255>

Description: Specify TTL for outgoing IP packets.
```

Range: < 2 to 255 >

udp-bcast-forward

- [no] ip udp-bcast-forward

```
Usage: [no] ip udp-bcast-forward

Description: Enable/disable UDP broadcast forwarding.
```

unreachable

- [no] ip icmp unreachable

```
Usage: [no] ip icmp unreachable

Description: Enable/disable destination unreachable error messages.
```

vlan

- ip source-binding *VLAN-ID*

Next Available Option:

- **ip** -- (IP-ADDR) **(p. 280)**

- [no] ip route *IP-ADDR/MASK-LENGTH* vlan *VLAN-ID*

```
Specify the destination VLAN.
```

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 276)**

zero-broadcast

- [no] ip zero-broadcast

```
Usage: [no] ip zero-broadcast

Description: Enable/disable usage of zero broadcast IP Address.
```

ipv6

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show ipv6 (page 482)** **ip (page 269)**

```
Usage: [no] ipv6 ...

Description: Configure various IP parameters for the VLAN. The 'ipv6'
             command must be followed by a feature-specific keyword.
             Use 'ipv6 ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

COMMAND STRUCTURE

- [no] ipv6 **authorized-managers** -- Define the IPV6 addresses allowed to manage the switch. **(p. 292)**
  - **IPV6-ADDR** -- Authorized manager IPv6 address. (IPV6-ADDR) **(p. 294)**
    - **access < Manager | Operator >** -- Define an access level desired. **(p. 291)**
    - **IPV6-MASK** -- IP mask defining a group of adjacent manager IP addresses. (IPV6-ADDR) **(p. 294)**
- [no] ipv6 **icmp** -- ICMPv6 rate limiting. **(p. 293)**
  - **error-interval** -- Send the ICMP error message. **(p. 293)**
    - **int < 0 to 2147483647 >** -- Specify interval-range. **(p. 293)**
      - **bucket-size** -- Set the bucket size. This is optional. **(p. 292)**
        - **int < 1 to 200 >** -- Specify bucket size. **(p. 293)**
- [no] ipv6 **nd** -- IPv6 neighbor discovery. **(p. 294)**
  - **dad-attempts** -- IPv6 neighbor discovery duplicate address detection. **(p. 292)**
    - **number < 0 to 600 >** -- Configures the number of neighbor solicitations to send when performing duplicate address detection **(p. 294)**

COMMAND DETAILS

access (p. 291)	**error-interval (p. 293)**	**IPV6-MASK (p. 294)**
authorized-managers (p. 292)	**icmp (p. 293)**	**nd (p. 294)**
bucket-size (p. 292)	**int (p. 293)**	**number (p. 294)**
dad-attempts (p. 292)	**IPV6-ADDR (p. 294)**	

access

- ipv6 authorized-managers *IPV6-ADDR* access *< Manager | Operator >*

```
Define an access level desired.
```

Supported Values:

- **Manager**
- **Operator**

authorized-managers

- [no] ipv6 authorized-managers

```
Usage: [no] ipv6 authorized-managers <IPV6-ADDR [IPV6-MASK]>
               access [manager|operator] [IPV6-MASK]

Description: Define the IPV6 addresses allowed to manage the switch.
             Clients using the specified IPV6 addresses are allowed
             to access the switch's web browser interface, telnet to
             the switch and to perform TFTP operations.
             A maximum of 10 addresses may be configured.

Parameters:

    o IPV6-ADDR - The IPV6 address of an authorized manager.

    o IPV6-MASK - A mask that allows you to define which portions of
      the listed IP address need to be matched by an incoming request.
      The default mask is ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
      For example, with an ipv6 authorized address of
      2001:db8:5:0:218:71ff:fec5:4400 and a mask of
      ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff,only access from
      2001:db8:5:0:218:71ff:fec5:4400 is allowed. With a mask of
      ffff:ffff:ffff:ffff:ffff:ffff:ffff:0, access from any IP address
      with 2001:db8:5:0:218:71ff:fec5:x is allowed.

    o [manager|operator] - A designation of the management capabilities
      that are accessible to the authorized manager.
      'manager' allows full access to all web browser and telnet to console
      for viewing and setting the switch configuration, and for performing
      all other interface operations,including all TFTP operations.
      'operator' allows view-only access from the web browser and the
      console, but does not allow changing the switch configuration or any
      TFTP operations. The default access level is manager.
```

Next Available Option:

- **IPV6-ADDR** -- Authorized manager IPv6 address. (IPV6-ADDR) **(p. 294)**

bucket-size

- ipv6 icmp error-interval *< 0 to 2147483647 >* bucket-size

```
This optional keyword specifies the maximum number of tokens allowed in the
token bucket at any time. Decreasing this value decreases the maximum number
of tokens that may be available at any time.
```

Range: 1-200

Default: 10

Next Available Option:

- **int** < 1 to 200 > -- Specify bucket size.**(p. 293)**

dad-attempts

- [no] ipv6 nd dad-attempts

```
This command is executed at the global config level. It configures the number
of neighbor solicitations to send when performing duplicate address detection
for a unicast address configured on a VLAN interface.
```

Range: 0-600 (0 = disabled)

Default: 3 (enabled)

Next Available Option:

- **number** < 0 to 600 > -- Configures the number of neighbor solicitations to send when performing duplicate address detection**(p. 294)**

error-interval

- [no] ipv6 icmp error-interval

```
Specifies the time interval in milliseconds between successive token adds.
Increasing this value decreases the rate at which tokens can be added. A
setting of zero disables ICMP messaging.
```

Range: 0 - 2147483647

Default: 100

Next Available Option:

- **int** < 0 to 2147483647 > -- Specify interval-range.**(p. 293)**

icmp

- [no] ipv6 icmp

```
ICMPv6 rate limiting.
```

Next Available Option:

- **error-interval** -- Send the ICMP error message.**(p. 293)**

int

- ipv6 icmp error-interval *< 0 to 2147483647 >*

```
Specify interval-range.
```

Range: < 0 to 2147483647 >

Next Available Option:

- **bucket-size** -- Set the bucket size. This is optional.**(p. 292)**

- ipv6 icmp error-interval *< 0 to 2147483647 >* bucket-size *< 1 to 200 >*

```
Specify bucket size.
```

Range: < 1 to 200 >

IPV6-ADDR

- ipv6 authorized-managers *IPV6-ADDR*

```
Authorized manager IPv6 address.
```

Next Available Options:

- **IPV6-MASK** -- IP mask defining a group of adjacent manager IP addresses. (IPV6-ADDR) **(p. 294)**
- **access** < Manager | Operator > -- Define an access level desired.**(p. 291)**

IPV6-MASK

- ipv6 authorized-managers *IPV6-ADDR IPV6-ADDR*

```
IP mask defining a group of adjacent manager IP addresses.
```

nd

- [no] ipv6 nd

```
IPv6 neighbor discovery. The Neighbor Discovery protocol operates in a manner
similar to the IPv4 ARP protocol to provide for the discovery of IPv6 devices
such as other switches, routers, management stations, and servers on the same
interface. It runs Duplicate Address Detection (DAD), locates alternate
routers, and many other IPv6 services.
```

Next Available Option:

- **dad-attempts** -- IPv6 neighbor discovery duplicate address detection.**(p. 292)**

number

- ipv6 nd dad-attempts *< 0 to 600 >*

```
Usage: ipv6 nd dad attempts <number>

Description: Configures the number of neighbor solicitations to send
when performing duplicate address detection.
```

Range: < 0 to 600 >

jumbo

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show jumbos (page 483)**

```
Usage: jumbo ...

Description: Configure Global Jumbos parameters for the switch.
```

NOTES

Restriction on Value of max-frame-size

The value of max-frame-size must be greater than or equal to 18 bytes more than the value selected for ip-mtu. For example, if ip-mtu is set to 8964, the max-frame-size is configured as 8982.

COMMAND STRUCTURE

- jumbo **ip-mtu** **< 1500 to 9198 >** -- Set the untagged Jumbos IP MTU or L3 MTU size for the switch **(p. 295)**
- jumbo **max-frame-size** **< 1518 to 9216 >** -- Set the untagged Jumbos Max frame size for the switch **(p. 295)**

COMMAND DETAILS

ip-mtu (p. 295)	**max-frame-size (p. 295)**

ip-mtu

- jumbo ip-mtu *< 1500 to 9198 >*

```
Usage: jumbo ip-mtu <1500-9198>

Description: Set the untagged Jumbos IP MTU or L3 MTU size for the switch.
             This value will be effective only when Jumbos are
           enabled. The value must be 18 bytes less than the value of max-frame-size.
```

Range: < 1500 to 9198 >

Default: 9198 bytes

max-frame-size

- jumbo max-frame-size *< 1518 to 9216 >*

```
Usage: jumbo max-frame-size <1518-9216>

Description: Set the untagged Jumbos Max frame size for the switch.
             This value will be effective only when Jumbos are
             enabled.
```

Range: < 1518 to 9216 >

Default: 9216 bytes

key-chain

OVERVIEW

Category:	Switch Security
Primary context:	config
Related Commands	**show key-chain (page 483)**

```
Usage: key-chain ASCII-STR
Usage: key-chain ASCII-STR key NUMBER [key-string ASCII-STR]
       [accept-lifetime <infinite|<<START-TIME|now> <END-TIME|duration SEC>>>]
       [send-lifetime <infinite|<<START-TIME|now> <END-TIME|duration SEC>>>]
Usage: no key-chain ASCII-STR
Usage: no key-chain ASCII-STR key KEY-ID

Description: Configures authentication key chains and individual keys.
             The configured key chains can be used for routing protocol
             authentication. Refer to routing protocol configuration
             commands for supported authentication methods and further
             instructions. The first form of command creates a new key
             chain unless the identified chain already exists.
             The second form of the command allows adding keys to an
             existent chain. The third and fourth forms of the command
             can be used to delete keys and chains.
             Parameters:
             - 'key-string ASCII-STR' authentication key to use
                (default empty string).
             - 'accept-lifetime ...' time and date when to start accepting
                the key and when the key is going to expire. The
                expiration time is set to 'infinite' by default.
             - 'send-lifetime ...' time and date when to start using
                the key to send and when the key is going to expire.
                A send key is always an accept key too. The expiration
                time is set to 'infinite' by default.
             Note: The 'accept-lifetime' period must always include the
             'send-lifetime' period. If only one of the periods is being
             changed then the other period also will be increased/reduced
             when it is necessary.
             Note: All time values are assumed to be GMT
```

COMMAND STRUCTURE

- [no] key-chain KEY-CHAIN **key** **< 0 to 255 >** -- Configure chain keys. (NUMBER) **(p. 311)**
  - **accept-lifetime** -- Set key accept lifetime. **(p. 301)**
    - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 301)**
      - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 316)**
        - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
            - **send-lifetime** -- Set key send lifetime. **(p. 314)**
              - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
                - *additional options available...*
              - **infinite** -- Set infinite lifetime. **(p. 310)**
              - **now** -- Use current day and time. **(p. 312)**
                - *additional options available...*
        - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

        - **send-lifetime** -- Set key send lifetime. **(p. 314)**
          - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
            - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
              - *additional options available...*
          - **infinite** -- Set infinite lifetime. **(p. 310)**
          - **now** -- Use current day and time. **(p. 312)**
            - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
  - **infinite** -- Set infinite lifetime. **(p. 310)**
    - **send-lifetime** -- Set key send lifetime. **(p. 314)**
      - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
        - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
          - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
            - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
          - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
      - **infinite** -- Set infinite lifetime. **(p. 310)**
      - **now** -- Use current day and time. **(p. 312)**
        - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
        - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
  - **now** -- Use current day and time. **(p. 312)**
    - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
      - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
        - **send-lifetime** -- Set key send lifetime. **(p. 314)**
          - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
            - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
              - *additional options available...*
          - **infinite** -- Set infinite lifetime. **(p. 310)**
          - **now** -- Use current day and time. **(p. 312)**
            - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
    - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
      - **send-lifetime** -- Set key send lifetime. **(p. 314)**
        - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
          - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
            - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
        - **infinite** -- Set infinite lifetime. **(p. 310)**
        - **now** -- Use current day and time. **(p. 312)**
          - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
            - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
          - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
- **key-string** -- Set key string (ASCII-STR) **(p. 312)**
  - **accept-lifetime** -- Set key accept lifetime. **(p. 301)**
    - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 301)**
      - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 316)**
        - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
            - **send-lifetime** -- Set key send lifetime. **(p. 314)**
              - *additional options available...*

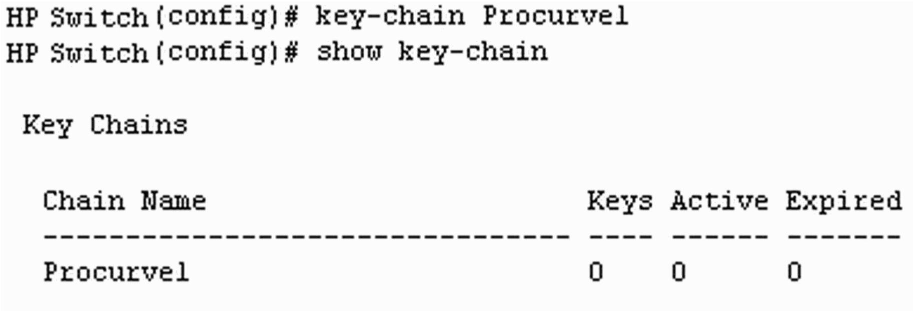
        - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
          - **send-lifetime** -- Set key send lifetime. **(p. 314)**
            - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **infinite** -- Set infinite lifetime. **(p. 310)**
            - **now** -- Use current day and time. **(p. 312)**
              - *additional options available...*
    - **infinite** -- Set infinite lifetime. **(p. 310)**
      - **send-lifetime** -- Set key send lifetime. **(p. 314)**
        - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
          - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
            - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
        - **infinite** -- Set infinite lifetime. **(p. 310)**
        - **now** -- Use current day and time. **(p. 312)**
          - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
            - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
          - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
    - **now** -- Use current day and time. **(p. 312)**
      - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
        - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
          - **send-lifetime** -- Set key send lifetime. **(p. 314)**
            - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **infinite** -- Set infinite lifetime. **(p. 310)**
            - **now** -- Use current day and time. **(p. 312)**
              - *additional options available...*
      - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
        - **send-lifetime** -- Set key send lifetime. **(p. 314)**
          - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
            - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
              - *additional options available...*
          - **infinite** -- Set infinite lifetime. **(p. 310)**
          - **now** -- Use current day and time. **(p. 312)**
            - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
              - *additional options available...*
            - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
  - **send-lifetime** -- Set key send lifetime. **(p. 314)**
    - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
      - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
        - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
        - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
    - **infinite** -- Set infinite lifetime. **(p. 310)**
    - **now** -- Use current day and time. **(p. 312)**
      - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
        - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
      - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
- **send-lifetime** -- Set key send lifetime. **(p. 314)**
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
    - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**
      - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**

      - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
    - **duration** -- Use current day and time. (NUMBER) **(p. 308)**
- **infinite** -- Set infinite lifetime. **(p. 310)**
- **now** -- Use current day and time. **(p. 312)**
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
    - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

EXAMPLES

Example: key-chain

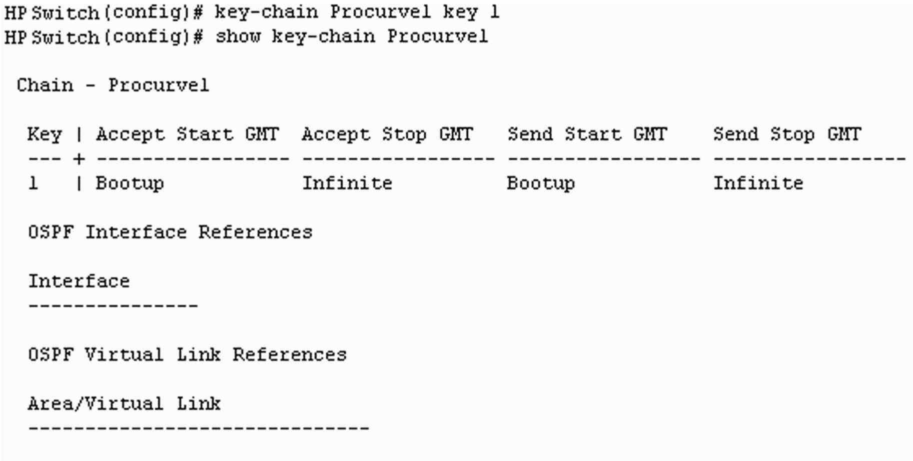
Generate a new key chain entry:



```
HP Switch(config)# key-chain Procurve1
HP Switch(config)# show key-chain

 Key Chains

  Chain Name                       Keys Active Expired
  -------------------------------- ---- ------ -------
  Procurve1                        0    0      0
```

Example: key-chain key

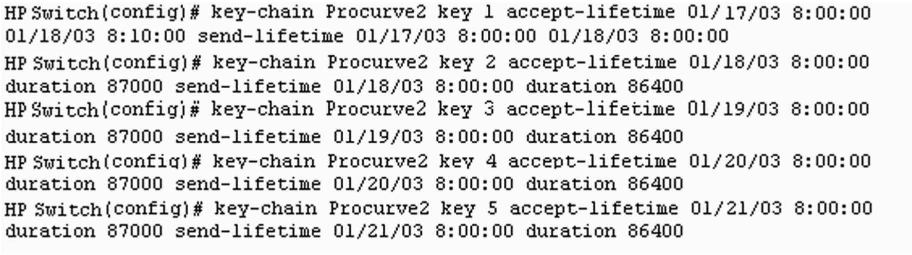
Generate a new time-independent key for the Procurve1 key chain entry:



```
HP Switch(config)# key-chain Procurve1 key 1
HP Switch(config)# show key-chain Procurve1

 Chain - Procurve1

  Key | Accept Start GMT  Accept Stop GMT   Send Start GMT    Send Stop GMT
  --- + ----------------- ----------------- ----------------- -----------------
  1   | Bootup            Infinite          Bootup            Infinite

  OSPF Interface References

  Interface
  ---------------

  OSPF Virtual Link References

  Area/Virtual Link
  ------------------------------
```

Example: key-chain key accept-lifetime

Add some keys to the key chain entry "Procurve2":



```
HP Switch(config)# key-chain Procurve2 key 1 accept-lifetime 01/17/03 8:00:00
01/18/03 8:10:00 send-lifetime 01/17/03 8:00:00 01/18/03 8:00:00
HP Switch(config)# key-chain Procurve2 key 2 accept-lifetime 01/18/03 8:00:00
duration 87000 send-lifetime 01/18/03 8:00:00 duration 86400
HP Switch(config)# key-chain Procurve2 key 3 accept-lifetime 01/19/03 8:00:00
duration 87000 send-lifetime 01/19/03 8:00:00 duration 86400
HP Switch(config)# key-chain Procurve2 key 4 accept-lifetime 01/20/03 8:00:00
duration 87000 send-lifetime 01/20/03 8:00:00 duration 86400
HP Switch(config)# key-chain Procurve2 key 5 accept-lifetime 01/21/03 8:00:00
duration 87000 send-lifetime 01/21/03 8:00:00 duration 86400
```

COMMAND DETAILS

accept-lifetime (p. 301)	**infinite (p. 310)**	**now (p. 312)**
date (p. 301)	**key (p. 311)**	**send-lifetime (p. 314)**
duration (p. 308)	**key-string (p. 312)**	**time (p. 316)**

accept-lifetime

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime

  `Set key accept lifetime.`

  Next Available Options:
  - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime

  `Set key accept lifetime.`

  Next Available Options:
  - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

date

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]*

  `Key accept start date.`

  Next Available Option:
  - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]*

  `Key accept stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]*

  ```
  Key accept stop date.
  ```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:

  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:

  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME] [DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE] [TIME] [DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]*

  ```
  Key accept start date.
  ```

  Next Available Option:
  - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key accept stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]*

  ```
  Key accept stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:

  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:

  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]* *[TIME]* *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:

  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:

- **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE]* *[TIME]* *[DATE]*

```
Key send stop date.
```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:

- **time** -- Key send start time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE]* *[TIME]* *[DATE]*

```
Key send stop date.
```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 316)**

duration

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

  Next Available Option:

  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

Next Available Option:

- **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME]* duration *NUMBER*

```
Use current day and time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now duration *NUMBER*

```
Use current day and time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE] [TIME]* duration *NUMBER*

```
Use current day and time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now duration *NUMBER*

```
Use current day and time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE] [TIME]* duration *NUMBER*

```
Use current day and time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now duration *NUMBER*

```
Use current day and time.
```

infinite

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime infinite

```
Set infinite lifetime.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime infinite

```
Set infinite lifetime.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime infinite

```
Set infinite lifetime.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime infinite

```
Set infinite lifetime.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite

```
Set infinite lifetime.
```

Next Available Option:

- **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite

  ```
  Set infinite lifetime.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime infinite

  ```
  Set infinite lifetime.
  ```

key

- [no] key-chain *KEY-CHAIN* key *< 0 to 255 >*

  ```
  Configure chain keys.
  ```

  Range: < 0 to 255 >

  Next Available Options:
  - **key-string** -- Set key string (ASCII-STR) **(p. 312)**
  - **accept-lifetime** -- Set key accept lifetime.**(p. 301)**
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

key-string

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING*

  ```
  Set key string
  ```

  Next Available Options:
  - **accept-lifetime** -- Set key accept lifetime.**(p. 301)**
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

now

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:
  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now

  ```
  Use current day and time.
  ```

Next Available Options:

- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
- **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now

  ```
  Use current day and time.
  ```

Next Available Options:

- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
- **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now

  ```
  Use current day and time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

send-lifetime

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:

  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:

  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime

  ```
  Set key send lifetime.
  ```

Next Available Options:

- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
- **now** -- Use current day and time.**(p. 312)**
- **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:

  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:

  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:

  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime

  ```
  Set key send lifetime.
  ```

  Next Available Options:

  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **now** -- Use current day and time.**(p. 312)**
  - **infinite** -- Set infinite lifetime.**(p. 310)**

time

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]* *[TIME]*

  ```
  Key accept start time.
  ```

  Next Available Options:

  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]*

  ```
  Key accept start time.
  ```

  Next Available Options:
  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]* send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

Next Available Options:

- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
- **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]* *[TIME]* duration *NUMBER* send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

  Next Available Option:

  - **send-lifetime** -- Set key send lifetime.**(p. 314)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]* *[TIME]* send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE]* *[TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:

  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 301)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 308)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE]* *[TIME]* *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now *[DATE]* *[TIME]*

  ```
  Key send stop time.
  ```

kill

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	show ssh (page 509) show telnet (page 514)

```
Usage: kill [SESSION_ID]

Description: Kill other active console, telnet, or ssh sessions.
             If no session ID is specified, all other active sessions
             are terminated.
```

COMMAND STRUCTURE

- kill session **< (Range unavailble) >** -- Kill other active console, telnet, or ssh sessions (p. 322)

EXAMPLES

Example: kill SESSION-ID

Display the currently active management sessions, then terminate one of the Telnet sessions:

```
ProCurve# show telnet

 Telnet Activity

  Session Privilege From            To
  ------- --------- --------------- ---------------
        1 Superuser Console
    **  2 Manager    10.132.193.146
        3 Manager    10.132.193.101

ProCurve# kill 3
ProCurve# show telnet

 Telnet Activity

  Session Privilege From            To
  ------- --------- --------------- ---------------
        1 Superuser Console
    **  2 Manager    10.132.193.146
```

COMMAND DETAILS

session (p. 322)

session

- kill *< (Range unavailble) >*

```
Usage: kill [SESSION_ID]

Description: Kill other active console, telnet, or ssh sessions.
```

```
If no session ID is specified, all other active sessions
are terminated.
```

Range: < (Range unavailble) >

licenses

OVERVIEW

Category:	
Primary context:	manager
Related Commands	**show licenses (page 484)**

```
Usage: licenses <hardware-id PKG-ID |
                 install PKG-ID PKG-KEY |
                 uninstall PKG-ID>

Description: Manage premium features.

Parameters:

    o hardware-id - Display the hardware ID for installing the specified
                    package on this chassis.
    o install     - Install the specified package.
    o uninstall   - Uninstall the specified package, and display the
                    uninstall verification key.
```

NOTES

Premium Features

The Premium License features are:

- OSPF
- PIM-DM (Dense Mode)
- PIM-SM (Sparse Mode)
- QinQ (Provider Bridging)
- VRRP

COMMAND STRUCTURE

- licenses **hardware-id** **< premium >** -- Display hardware ID for installation request. **(p. 324)**
- licenses **install** **< premium >** -- Install the specified package. **(p. 325)**
  - **key** -- Enter key for this feature. (ASCII-STR) **(p. 325)**
- licenses **uninstall** **< premium >** -- Uninstall the specified package. **(p. 325)**

COMMAND DETAILS

hardware-id (p. 324)	**key (p. 325)**
install (p. 325)	**uninstall (p. 325)**

hardware-id

- licenses hardware-id *< premium >*

```
Display hardware ID for installation request.
```

Supported Values:

- **premium** -- key

install

- licenses install *< premium >*

```
Install the specified package.
```

Supported Values:

- **premium** -- key

Next Available Option:

- **key** -- Enter key for this feature. (ASCII-STR) **(p. 325)**

key

- licenses install *< premium > KEY*

```
Enter key for this feature.
```

uninstall

- licenses uninstall *< premium >*

```
Uninstall the specified package.
```

Supported Values:

- **premium** -- key

link-keepalive

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: link-keepalive interval <10-100>
       link-keepalive retries <3-10>

Description: Configure UDLD on your switch.
             The first version of the command is used to configure
             keep-alive interval in seconds. Here 10 is 1 sec, 11 is 1.1 sec,
             and so on. Default keep-alive interval is 5 seconds.
             The second version of the command is used to configure
             maximum number of keep-alive attempts. Default keep-alive
             attempt is 4.
```

COMMAND STRUCTURE

- link-keepalive **interval** **< 10 to 100 >** -- Set link keep-alive interval in deciseconds. **(p. 326)**
- link-keepalive **retries** **< 3 to 10 >** -- Set maximum number of link keep-alive attempts. **(p. 326)**

COMMAND DETAILS

interval (p. 326)	**retries (p. 326)**

interval

- link-keepalive interval *< 10 to 100 >*

```
Set link keep-alive interval in deciseconds.
```

Range: < 10 to 100 >

retries

- link-keepalive retries *< 3 to 10 >*

```
Set maximum number of link keep-alive attempts.
```

Range: < 3 to 10 >

link-test

OVERVIEW

Category:	
Primary context:	operator
Related Commands	**ping (page 367)**

```
Usage: link-test MAC-ADDR [vlan <VLAN-ID>] [repetitions <1-999>]
                          [timeout <1-256>]

Description: Test the connection to a MAC address on the LAN.
             The command sends a 802.2 test packet to a specific target
             node on a network directly attached to a port in that
             LAN. The target node must be able to respond to this test
             packet with an 802.2 Test Response packet in order for the
             test to work. The switch produces the following output if
             the link test succeeds: 'Link-test passed'; otherwise, the
             following is displayed: 'Link-test timed out'.

Parameters:

    o MAC-ADDR - MAC address of the device to which to send link test.

    o [vlan VLAN-ID] - VLAN on which the device is expected to be present.
      If this argument is not present, VLAN 1 will be used.

    o [repetitions <1-999>] - Number of test packets to send; the
      default value is 1.

    o [timeout <1-256>] - Seconds within which a response is required
      before the test is considered as failed; the default value is 5.

Examples:

    (1) hp-switch# link-test 0800095F3AD6
```

COMMAND STRUCTURE

- link-test **mac** -- MAC address of device to which to send link test. (MAC-ADDR) **(p. 328)**
- link-test **repetitions < 1 to 999 >** -- Number of test packets to send <1-999>. (NUMBER) **(p. 328)**
- link-test **timeout < 0 to 256 >** -- Test timeout in seconds <0-256>. (NUMBER) **(p. 328)**
- link-test **vlan** -- VLAN where the device to be tested is present. (VLAN-ID) **(p. 328)**

EXAMPLES

Example: link-test

Test the link to MAC address 0800095F3AD6 on VLAN 1:

```
ProCurve# link-test 0800095F3AD6
```

COMMAND DETAILS

mac

- link-test *MAC-ADDR*

```
MAC address of device to which to send link test.
```

repetitions

- link-test repetitions *< 1 to 999 >*

```
Number of test packets to send <1-999>.
```

Range: < 1 to 999 >

timeout

- link-test timeout *< 0 to 256 >*

```
Test timeout in seconds <0-256>.
```

Range: < 0 to 256 >

vlan

- link-test vlan *VLAN-ID*

```
VLAN where the device to be tested is present.
```

lldp

OVERVIEW

Category:	Device Discovery
Primary context:	config
Related Commands	**show lldp (page 485)**

```
Usage:lldp ...

Description: Configuration for LLDP parameter. Provides a standards-based method
             for enabling the switches to advertise themselves to adjacent devices
             and to learn about adjacent LLDP devices.
             You can also configure the Media Extension Discovery (MED) extension
             to LLDP for Voice over IP (VoIP) devices.
```

COMMAND STRUCTURE

- lldp **admin-status** -- Set the port in one of the operational mode transmit | receive | transmit & receive | disable the port ([ethernet] PORT-LIST) **(p. 331)**
  - **omodes < TxOnly | RxOnly | Tx_Rx | ... >** -- Set the operational mode: transmit | receive | transmit-receive | disable. (NUMBER) **(p. 335)**
- [no] lldp **auto-provision** -- Configure various parameters related to lldp automatic provisioning **(p. 331)**
  - **radio-ports** -- Configure various parameters related to automatic provisioning for the radio-port application **(p. 335)**
    - **auto-vlan** -- Create a VLAN, with the specified VLAN id value, to be used as the radio-ports controller auto-generated VLAN. **(p. 331)**
      - **auto-vlan < 2 to 4094 >** -- Create a VLAN, with the specified VLAN id value, to be used as the radio-ports controller auto-generated VLAN. (VLAN-ID) **(p. 331)**
        - **auto** -- **(p. 331)**
    - **vlan-base < 2 to 4094 >** -- Assign the default value of the VLAN id to be used if an auto-generated VLAN is created for a radio-port application. (VLAN-ID) **(p. 336)**
- [no] lldp **config** -- Specify configurational parameters to the port ([ethernet] PORT-LIST) **(p. 333)**
  - **basicTlvEnable < port_descr | system_name | system_descr | ... >** -- Specify the Basic TLV List to be advertised. (NUMBER) **(p. 332)**
  - **dot1TlvEnable** -- Specify the 802.1 TLV List to be advertised. **(p. 333)**
    - **vlan-name** -- Specify that the VLAN name TLV is to be advertised. **(p. 336)**
  - **dot3TlvEnable < macphy_config >** -- Specify the 802.3 TLV List to be advertised. (NUMBER) **(p. 334)**
  - **ipAddrEnable** -- Set IP ADDR to be enabled. (IP-ADDR) **(p. 334)**
  - **medPortLocation** -- Configure location-id information to be advertised. **(p. 334)**
    - **civic-addr** -- Specify the civic location-id information to be advertised **(p. 332)**
      - **COUNTRY** -- Specify the Country Code of two characters. (ASCII-STR) **(p. 333)**
        - **WHAT** -- Specify the 'what' number of range <0-2>. (NUMBER) **(p. 336)**
          - **CA-TYPE** -- Specify the ca-type value of range <0-255>. (NUMBER) **(p. 332)**
            - **CA-VALUE** -- Specify the ca-value string. (ASCII-STR) **(p. 332)**
    - **elin-addr** -- Specify the elin address location to be advertised. **(p. 334)**
      - **addr** -- Specify the Location name to be advertised. (OCTET-STR) **(p. 331)**
  - **medTlvEnable < capabilities | network_policy | location_id | ... >** -- Specify the MED TLV List to be advertised. (NUMBER) **(p. 335)**

- [no] lldp **enable-notification** -- Set the port for which notification should be enabled ([ethernet] PORT-LIST) **(p. 334)**
- lldp **fast-start-count < 1 to 10 >** -- Set MED fast-start count in seconds (NUMBER) **(p. 334)**
- lldp **holdtime-multiplier < 2 to 10 >** -- Set holdtime-multipler between <2-10>; the default is 4 (NUMBER) **(p. 334)**
- lldp **refresh-interval < 5 to 32768 >** -- Set refresh interval/transmit-interval in seconds (NUMBER) **(p. 335)**
- [no] lldp **run** -- Start or Stop LLDP on device **(p. 336)**
- [no] lldp **top-change-notify** -- Set the port for which LLDP MED topology notification should be enabled ([ethernet] PORT-LIST) **(p. 336)**

EXAMPLES

Example: lldp config basicTlvEnable

Exclude the system name from the outbound LLDP advertisements for all ports:

```
ProCurve(config)# no lldp config A1-A24 basicTlvEnable system_name
```

Example: lldp config ipAddrEnable

Use a secondary IP address in LLDP advertisements. In this example, use secondary IP address 10.10.10.100, which is on a subnetted VLAN that contains port 3:

```
ProCurve(config)# lldp config 3 ipAddrEnable 10.10.10.100
```

Example: lldp enable-notification

Enable SNMP notification on ports 1 - 5:

```
ProCurve(config)# lldp enable-notification A1-A5
```

Example: lldp holdtime-multiplier

If the refresh interval on the switch is 15 seconds and the holdtime multiplier is at the default, the Time-to-Live for advertisements transmitted from the switch is 60 seconds (4 * 15). To reduce the Time-to-Live, lower the holdtime-interval to 2, which results in a Time-to-Live of 30 seconds:

```
ProCurve(config)# lldp holdtime-multiplier 2
```

Example: lldp run

Disable LLDP on the switch:

```
ProCurve(config)# no lldp run
```

COMMAND DETAILS

config (p. 333)	medTlvEnable (p. 335)

addr

- lldp config *[ETHERNET] PORT-LIST* medPortLocation elin-addr *OCTET-STR*

```
Specify the Location name to be advertised.
```

admin-status

- lldp admin-status *[ETHERNET] PORT-LIST*

```
Usage: lldp admin-status <port-list> <txonly | rxonly
                                      tx_rx | disable>

Description: Set the port in one of the operational mode
             transmit | receive | transmit & receive |
             disable the port.
```

Next Available Option:

- **omodes** < TxOnly | RxOnly | Tx_Rx | ... > -- Set the operational mode: transmit | receive | transmit-receive | disable. (NUMBER) **(p. 335)**

auto

- lldp auto-provision radio-ports auto-vlan *< 2 to 4094 >* auto

auto-provision

- lldp auto-provision

```
Usage:[no] lldp auto-provision radio-ports [suggested-auto-vlan|auto-vlan]
                                           <vid>

Description: Configure various parameters related to lldp automatic
             provisioning.
```

Next Available Option:

- **radio-ports** -- Configure various parameters related to automatic provisioning for the radio-port application**(p. 335)**

auto-vlan

- [no] lldp auto-provision radio-ports auto-vlan

```
Create a VLAN, with the specified VLAN id value, to be used as
the radio-ports controller auto-generated VLAN.
```

Next Available Option:

- **auto-vlan** < 2 to 4094 > -- Create a VLAN, with the specified VLAN id value, to be used as the radio-ports controller auto-generated VLAN. (VLAN-ID) **(p. 331)**

- lldp auto-provision radio-ports auto-vlan *< 2 to 4094 >*

```
Create a VLAN, with the specified VLAN id value, to be used as
the radio-ports controller auto-generated VLAN.
```

Range: < 2 to 4094 >

Next Available Option:

- **auto** -- **(p. 331)**

basicTlvEnable

- [no] lldp config *[ETHERNET] PORT-LIST* basicTlvEnable *< port_descr | system_name | system_descr | ... >*

```
Specify the Basic TLV List to be advertised.
```

Supported Values:

- **port_descr** -- Port Description TLV
- **system_name** -- System Name TLV
- **system_descr** -- System Description TLV
- **system_cap** -- System Capability TLV

CA-TYPE

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY NUMBER NUMBER*

```
Specify the ca-type value of range <0-255>.
```

Next Available Option:

- **CA-VALUE** -- Specify the ca-value string. (ASCII-STR) **(p. 332)**

CA-VALUE

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY NUMBER NUMBER CA-VALUE*

```
Specify the ca-value string.
```

civic-addr

- [no] lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr

```
Usage: lldp config <port-list> medPortLocation civic-str <COUNTRY-STR>
                                  <WHAT> <CA-TYPE> <CA-VALUE>

Description: Specify the civic location-id information to be advertised.
             The total length of the TLV is 104.
             COUNTRY-STR : Set the Country Code of two characters.e.g. DE or US.
             WHAT        : Set the 'what' number of range <0-2>.
                           0 - Location of DHCP server.
                           1 - Location of Switch.
                           2 - Location of Client.
             CA-TYPE     : Set the ca-type of range <0-255>.
                           It is a repeatable parameter.ca-type should be unique.
                           ca-type sholud be followed by ca-value.
             CA-VALUE    : Set the ca-value string.
```

Next Available Option:

- **COUNTRY** -- Specify the Country Code of two characters. (ASCII-STR) **(p. 333)**

config

- lldp config *[ETHERNET] PORT-LIST*

```
Usage: [no] lldp config <PORT-LIST> <basicTlvEnable TLVMAP |
                                     dot1TlvEnable vlan-name |
                                     dot3TlvEnable  TLVMAP |
                                     ipAddrEnable IP-ADDR  |
                                     medPortLocation ...   |
                                     medTlvEnable   TLVMAP>

Description: Specify configurational parameters to the port.
             Set basicTlvEnable with any one of the following TLV Maps.
                 port_descr     : Send Port Description TLV out this port.
                 system_name    : Send System Name TLV out this port.
                 system_descr   : Send System Descr TLV out this port.
                 system_cap     : Send Capability TLV out this port.
             Set dot1TlvEnable with the following TLVs.
                 vlan_name      : Enable VLAN name TLV out the given port(s).
             Set dot3TlvEnable with the following TLV Map.
                 macphy_config  : Send Mac Phy Config TLV out this port.
             Set ipAddrEnable with the IP-ADDR to send out this port.
             Set medPortLocation with location information for the port.
                 civic-addr     : Set civic address to send out this port.
                 elin-addr      : Set elin address to send out this port.
             Set medTlvEnable with any one of the following TLV Maps.
                 capabilities   : Send Capability TLV out this port.This TLV has
                                  to be enabled first to enable any MED TLV's.
                 network_policy : Send Network Policy TLV out this port.
                 location_id    : Send Location Id TLV out this port.
                 poe            : Send Med Poe TLV out this port.
```

Next Available Options:

- **basicTlvEnable** < port_descr | system_name | system_descr | ... > -- Specify the Basic TLV List to be advertised. (NUMBER) **(p. 332)**
- **ipAddrEnable** -- Set IP ADDR to be enabled. (IP-ADDR) **(p. 334)**
- **dot1TlvEnable** -- Specify the 802.1 TLV List to be advertised.**(p. 333)**
- **medTlvEnable** < capabilities | network_policy | location_id | ... > -- Specify the MED TLV List to be advertised. (NUMBER) **(p. 335)**
- **medPortLocation** -- Configure location-id information to be advertised. **(p. 334)**
- **dot3TlvEnable** < macphy_config > -- Specify the 802.3 TLV List to be advertised. (NUMBER) **(p. 334)**

COUNTRY

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY*

```
Specify the Country Code of two characters.
```

Next Available Option:

- **WHAT** -- Specify the 'what' number of range <0-2>. (NUMBER) **(p. 336)**

dot1TlvEnable

- lldp config *[ETHERNET] PORT-LIST* dot1TlvEnable

```
Specify the 802.1 TLV List to be advertised.
```

Next Available Option:

- **vlan-name** -- Specify that the VLAN name TLV is to be advertised. **(p. 336)**

dot3TlvEnable

- [no] lldp config *[ETHERNET] PORT-LIST* dot3TlvEnable *< macphy_config >*

```
Specify the 802.3 TLV List to be advertised.
```

Supported Values:

- **macphy_config** -- MAC Physical Config Tlv

elin-addr

- [no] lldp config *[ETHERNET] PORT-LIST* medPortLocation elin-addr

```
Specify the elin address location to be advertised.
```

Next Available Option:

- **addr** -- Specify the Location name to be advertised. (OCTET-STR) **(p. 331)**

enable-notification

- [no] lldp enable-notification *[ETHERNET] PORT-LIST*

```
Usage: [no] lldp notificationEnable <PORT-LIST>

Description: Set the port for which notification should be enabled.
```

fast-start-count

- lldp fast-start-count *< 1 to 10 >*

```
Usage: lldp fast-start-count <1-10>

Description: Set MED fast-start count in seconds.
```

Range: < 1 to 10 >

holdtime-multiplier

- lldp holdtime-multiplier *< 2 to 10 >*

```
Usage: lldp holdtime-multiplier <2-10>

Description: Set holdtime-multipler between <2-10>; the default is 4.
```

Range: < 2 to 10 >

ipAddrEnable

- [no] lldp config *[ETHERNET] PORT-LIST* ipAddrEnable *IP-ADDR*

```
Set IP ADDR to be enabled.
```

medPortLocation

- [no] lldp config *[ETHERNET] PORT-LIST* medPortLocation

```
Configure location-id information to be advertised.
```

Next Available Options:

- **civic-addr** -- Specify the civic location-id information to be advertised**(p. 332)**
- **elin-addr** -- Specify the elin address location to be advertised. **(p. 334)**

medTlvEnable

- [no] lldp config *[ETHERNET] PORT-LIST* medTlvEnable *< capabilities | network_policy | location_id | ... >*

```
Specify the MED TLV List to be advertised.
```

Supported Values:

- **capabilities** -- Capability TLV
- **network_policy** -- Network Policy TLV
- **location_id** -- Location Id TLV
- **poe** -- Poe TLV

omodes

- lldp admin-status *[ETHERNET] PORT-LIST < TxOnly | RxOnly | Tx_Rx | ... >*

```
Set the operational mode: transmit | receive |
transmit-receive | disable.
```

Supported Values:

- **TxOnly** -- Set in transmit mode.
- **RxOnly** -- Set in receive mode.
- **Tx_Rx** -- Set in transmit & Receive mode.
- **disable** -- disable.

radio-ports

- [no] lldp auto-provision radio-ports

```
Usage:[no] lldp auto-provision radio-ports [suggested-auto-vlan|auto-vlan]
                                           <vid>

Description: Configure various parameters related to automatic
             provisioning for the radio-port application.
             If no additional parameters following the radio-ports
             parameter this command will enable the auto-provision
             option (use the [no] keyword to disable the
             auto-provision option).
```

Next Available Options:

- **auto-vlan** -- Create a VLAN, with the specified VLAN id value, to be used as the radio-ports controller auto-generated VLAN. **(p. 331)**
- **vlan-base** < 2 to 4094 > -- Assign the default value of the VLAN id to be used if an auto-generated VLAN is created for a radio-port application. (VLAN-ID) **(p. 336)**

refresh-interval

- lldp refresh-interval *< 5 to 32768 >*

```
Usage: lldp refresh-interval <5-32768>

Description: Set refresh interval/transmit-interval in seconds.
             The default is 30.
             The refresh interval/transmit-interval should be greater
             than or equal to (4*delay-interval).
             The default value of delay-interval is 2.
```

Range: < 5 to 32768 >

run

- [no] lldp run

```
Usage:[no] lldp run

Description: Start or Stop LLDP on device.
```

top-change-notify

- [no] lldp top-change-notify *[ETHERNET] PORT-LIST*

```
Usage:[no] lldp top-change-notify <port-list>

Description: Set the port for which LLDP MED topology notification should be enabled.
```

vlan-base

- lldp auto-provision radio-ports vlan-base *< 2 to 4094 >*

```
Assign the default value of the VLAN id to be used if an
auto-generated VLAN is created for a radio-port application.
```

Range: < 2 to 4094 >

vlan-name

- [no] lldp config *[ETHERNET] PORT-LIST* dot1TlvEnable vlan-name

```
Specify that the VLAN name TLV is to be advertised. Enables LLDP VLAN TLV advertisements
 on an
individual port or range of ports. The advertisements are sent out each configured
port at the
configured frequency. The default frequency is every 30 seconds.
Note: To change the default frequency, use the "lldp refresh-interval" command.
```

WHAT

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY NUMBER*

```
Specify the 'what' number of range <0-2>.
```

Next Available Option:

- **CA-TYPE** -- Specify the ca-type value of range <0-255>. (NUMBER) **(p. 332)**

lockout-mac

OVERVIEW

Category:	Port Security
Primary context:	config
Related Commands	**show lockout-mac (page 486)**

```
Usage: lockout-mac <MAC-ADDR>

Description: Lock out a MAC address.

Parameter:

    o MAC-ADDR  - MAC address to lock down.

Examples:

    (1) hp-switch#  lockout-mac 0800095F3AD6
```

COMMAND STRUCTURE

EXAMPLES

Example: lockout-mac

Drop all traffic to or from MAC address 0800095F3AD6:

```
ProCurve# lockout-mac 0800095F3AD6
```

log

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**logging (page 340)** **show logging (page 486)**

```
Usage: log [-a|-r|-m|-p|-w|-i|-d|substring ...]

Description: Display log events.
             -a - Instructs the switch to display all recorded log
             events, which includes events from previous boot cycles.
             -r - Instructs the switch to display recorded
             log events in reverse order (most recent first).
             substring - Instructs the switch to display
             only those events that match the substring.

             The remaining event class options (listed below in
             order of severity - lowest severity first) confine
             output to event clases of equal or higher severity
             -d - Debug
             -i - Informative
             -w - Warnings
             -p - Performance
             -m - Major
             Only one of options -d,-i,-w,-p and -m may be specified.

             The -a, -r, and substring options may be used in
             combination with an event class option.
```

COMMAND STRUCTURE

- log **-a** -- Display all log events, including those from previous boot cycles. **(p. 338)**
- log **event_class < -M | -P | -W | ... >** -- Specify substring to match in log entry. See 'log help' for details. **(p. 338)**
- log **option** -- Specify substring to match in log entry. See 'log help' for details. (ASCII-STR) **(p. 339)**
- log **-r** -- Display log events in reverse order (most recent first). **(p. 339)**

COMMAND DETAILS

-a (p. 338)	**option (p. 339)**
event_class (p. 338)	**-r (p. 339)**

-a

- log -a

```
Display all log events, including those from previous boot cycles.
```

event_class

- log

```
Specify substring to match in log entry. See 'log help' for details.
```

Supported Values:

- **-M** -- Major event class.
- **-P** -- Performance event class.
- **-W** -- Warning event class.
- **-I** -- Information event class.
- **-D** -- Debug event class.

option

- log *OPTION*

```
Specify substring to match in log entry. See 'log help' for details.
```

-r

- log -r

```
Display log events in reverse order (most recent first).
```

logging

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**log (page 338)** **show logging (page 486)**

```
Usage: [no] logging <IP-ADDR>
       [no] logging facility <facility>
       [no] logging severity <severity>
       [no] logging system-module <module>

Description: Add an IP address to the list of receiving syslog servers.
             Use of 'no' without an IP address specified will remove all
             IP addresses from the list of syslog receivers. If an IP
             address is specified, that receiver will be removed.
             - Specify syslog server facility with <facility>. 'no
             logging facility <facility>' sets facility back to defaults.
             - Specify severity for event messages to be filtered to the
             syslog server with <severity>. 'no logging severity
             <severity>' sets severity back to default.
             - Event messages of specified system module will be sent to
             the syslog server. 'no' sends messages from all system
             modules. Messages are 1st filtered by selected severity.
```

NOTES

Maximum Number of Entries

Starting in software release K.13.xx, the maximum number of entries supported in the Event Log is increased from 1000 to 2000 entries. Entries are listed in chronological order, from the oldest to the most recent. Once the log has received 2000 entries, it discards the oldest message each time a new message is received. The Event Log window contains 14 log entry lines. You can scroll through it to view any part of the log.

COMMAND STRUCTURE

- [no] logging **facility** **< kern | user | mail | ... >** -- Specify the syslog facility value that will be used for all syslog servers **(p. 341)**
- [no] logging **ip-address** -- Add an IP address to the list of receiving syslog servers (IP-ADDR) **(p. 341)**
- [no] logging **severity** **< major | error | warning | ... >** -- Event messages of the specified severity or higher will be sent to the syslog server **(p. 342)**
- [no] logging **system-module** **< all-pass | vlan | ip | ... >** -- Event messages of the specified system module (subsystem) will be sent to the syslog server **(p. 342)**

COMMAND DETAILS

facility (p. 341)	**severity (p. 342)**
ip-address (p. 341)	**system-module (p. 342)**

facility

- [no] logging facility *< kern | user | mail | ... >*

```
Usage: [no] logging facility <facility>

Description: Specify the syslog facility value that will be used
             for all syslog servers. Syslog facility determines
             where syslog servers should log the syslog message.
```

Supported Values:

- **kern**
- **user**
- **mail**
- **daemon**
- **auth**
- **syslog**
- **lpr**
- **news**
- **uucp**
- **sys9**
- **sys10**
- **sys11**
- **sys12**
- **sys13**
- **sys14**
- **cron**
- **local0**
- **local1**
- **local2**
- **local3**
- **local4**
- **local5**
- **local6**
- **local7**

ip-address

- [no] logging *IP-ADDR*

```
Usage: [no] logging <IP-ADDR>
       [no] logging facility <facility>
       [no] logging severity <severity>
       [no] logging system-module <module>

Description: Add an IP address to the list of receiving syslog servers.
             Use of 'no' without an IP address specified will remove all
             IP addresses from the list of syslog receivers. If an IP
             address is specified, that receiver will be removed.
             - Specify syslog server facility with <facility>. 'no
             logging facility <facility>' sets facility back to defaults.
             - Specify severity for event messages to be filtered to the
             syslog server with <severity>. 'no logging severity
             <severity>' sets severity back to default.
             - Event messages of specified system module will be sent to
             the syslog server. 'no' sends messages from all system
             modules. Messages are 1st filtered by selected severity.
```

severity

- [no] logging severity *< major | error | warning | ... >*

```
Usage: [no] logging severity <severity>

Description: Event messages of the specified severity or higher will be
             sent to the syslog server. 'no' sends all severities.
```

Supported Values:

- **major**
- **error**
- **warning**
- **info**
- **debug**

system-module

- [no] logging system-module *< all-pass | vlan | ip | ... >*

```
Usage: [no] logging system-module <module>

Description: Event messages of the specified system module (subsystem)
             will be sent to the syslog server. 'no' sends messages
             from all system modules, as does 'logging system-module
             all-pass'. Messages are severity filtered before
             system module filtering occurs.
```

Supported Values:

- **all-pass**
- **vlan**
- **ip**
- **igmp**
- **ipx**
- **stp**
- **system**
- **chassis**
- **console**
- **ports**
- **dhcp**
- **download**
- **tcp**
- **telnet**
- **timep**
- **tftp**
- **Xmodem**
- **update**
- **mgr**
- **system**
- **snmp**
- **addrMgr**
- **pagp**
- **fault**
- **ldbal**
- **garp**
- **gvrp**
- **cos**

- **lacp**
- **dhcpr**
- **stack**
- **dma**
- **SNTP**
- **802.1x**
- **cdp**
- **auth**
- **tacacs**
- **radius**
- **ssh**
- **NETINET**
- **OSPF**
- **XRRP**
- **ssl**
- **IpAddrMgr**
- **MacAuth**
- **KMS**
- **PIM**
- **maclock**
- **ACL**
- **udpf**
- **inst-mon**
- **udld**
- **HPESP**
- **lldp**
- **connfilt**
- **RateLim**
- **idm**
- **IPLOCK**
- **dhcp-snoop**
- **vrrp**
- **usb**
- **licensing**
- **loop-protect**
- **sFlow**
- **arp-protect**
- **dhcpv6c**
- **mtm**
- **mld**
- **dca**
- **QinQ**
- **autorun**
- **ffi**
- **wsm**

log-numbers

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] log-numbers

Description: Enable the display of log event numbers when log is displayed
             via the CLI or via the menu.
```

COMMAND STRUCTURE

logout

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	

```
Usage: logout

Description: Terminate this console/telnet session.
```

COMMAND STRUCTURE

loop-protect

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] loop-protect <...>
            [[ethernet] PORT-LIST [receiver-action <send-disable|no-disable>]|
            [transmit-interval <1-10>]|
            [disable-period <0-604800>]|
            [trap <loop-detected>]

Description: Configure Loop protection on the switch.


Parameters:
 o ethernet PORT-LIST - Port(s) to configure loop protection on. By default
                        loop protection is disabled on a port
 o receiver-action    - Sets the loop detected action per port. When a loop
                        is detected the port that received the loop protection
                        packet determines the action taken. If send-disable
                        is selected the port that transmitted the packet will
                        be disabled. If no-disable is selected, the port will
                        not be disabled. The default action is 'send-disable'.
 o trap <loop-detected> - Configure Loop protection traps. The following
                          traps are generated by Loop protection
                        - 'loop-detected' signifies that a loop was detected
                           on a port.
 o disable-timer <0-604800> (default:0) - Sets the time in seconds to
                        disable a port for when a loop has been detected. A
                        value of 0 disables the auto reenable functionality.
                        By default the timer is disabled.

 o transmit-interval <1-10> (default:5) - Time in seconds between transmission
                                          of loop protection packets.
```

COMMAND STRUCTURE

- loop-protect **disable-timer < 0 to 604800 >** -- Set time in seconds to wait before attempting to reenable a port. (NUMBER) **(p. 347)**
- [no] loop-protect **port-list** -- Specify the ports that are to be added to/removed from loop protection. ([ethernet] PORT-LIST) **(p. 347)**
  - **receiver-action < send-disable | no-disable >** -- Select action to take when loop protect packets are received on the specified port(s). **(p. 347)**
- loop-protect **transmit-interval < 1 to 10 >** -- Set time between packet transmissions. (NUMBER) **(p. 347)**
- [no] loop-protect **trap** -- Specify loop protection traps that are to be enabled/disabled. **(p. 347)**
  - **loop-detected** -- generate trap when a loop is detected **(p. 347)**

COMMAND DETAILS

disable-timer (p. 347)	**port-list (p. 347)**	**transmit-interval (p. 347)**
loop-detected (p. 347)	**receiver-action (p. 347)**	**trap (p. 347)**

disable-timer

- loop-protect disable-timer *< 0 to 604800 >*

  ```
  Set time in seconds to wait before attempting to reenable a port.
  ```

  Range: < 0 to 604800 >

loop-detected

- [no] loop-protect trap loop-detected

  ```
  generate trap when a loop is detected
  ```

port-list

- [no] loop-protect *[ETHERNET] PORT-LIST*

  ```
  Specify the ports that are to be added to/removed from loop protection.
  ```

  Next Available Option:
  - **receiver-action** < send-disable | no-disable > -- Select action to take when loop protect packets are received on the specified port(s). **(p. 347)**

receiver-action

- loop-protect *[ETHERNET] PORT-LIST* receiver-action *< send-disable | no-disable >*

  ```
  Select action to take when loop protect packets are received on the specified port(s).
  ```

  Supported Values:
  - **send-disable**
  - **no-disable**

transmit-interval

- loop-protect transmit-interval *< 1 to 10 >*

  ```
  Set time between packet transmissions.
  ```

  Range: < 1 to 10 >

trap

- [no] loop-protect trap

  ```
  Specify loop protection traps that are to be enabled/disabled.
  ```

  Next Available Option:
  - **loop-detected** -- generate trap when a loop is detected**(p. 347)**

mac-age-time

OVERVIEW

Category:	Device Discovery
Primary context:	config
Related Commands	

```
Usage: mac-age-time <60-999960>

Description: Set the MAC address table's age-out interval.
             A MAC address that is dynamically learned by the switch, stays
             in the switch's address table for a certain amount of time -
             the age-out interval, before being aged out. An address is aged
             out if the switch does not receive traffic from that MAC
             address for the age-out interval. The interval is measured in
             seconds. The default value is 300 seconds.
```

COMMAND STRUCTURE

EXAMPLES

Example: mac-age-time SECONDS

Configure the MAC age-out interval to seven minutes:

```
ProCurve(config)# mac-age-time 420
```

management-vlan

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show vlan (page 518)**

```
Usage: [no] management-vlan VLAN-ID
```

```
Description: Set the VLAN that is to be used as the management VLAN.
```

COMMAND STRUCTURE

EXAMPLES

Example: management-vlan

Set VLAN 100 as the management VLAN and add ports A1 and A2 to it:

```
ProCurve(config)# management-vlan 100
ProCurve(config)# vlan 100 tagged a1
ProCurve(config)# vlan 100 tagged a2
```

max-vlans

OVERVIEW

Category:	VLANs
Primary context:	config
Related Commands	

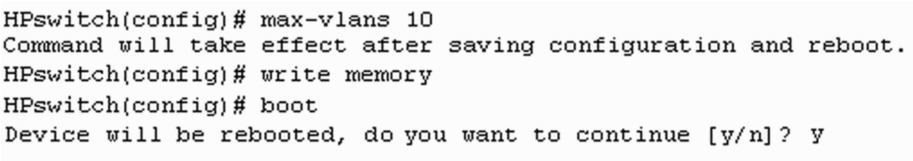
```
Usage: max-vlans <1-2048>

Description: Set the maximum number of VLANs on the switch.
             The default is 256.
```

COMMAND STRUCTURE

EXAMPLES

Example: max-vlans NUMBER

Reconfigure the switch to allow 10 VLANs:



```
HPswitch(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

menu

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	

```
Usage: menu

Description: Change console user interface to menu system.
```

COMMAND STRUCTURE

EXAMPLES

menu

Enter the menu mode for switch configuration:

```
ProCurve# menu

HP ProCurve Switch 5400zl                           1-Jan-2006   4:55:06
=======================- TELNET - MANAGER MODE -========================
                                   Main Menu

   1. Status and Counters...
   2. Switch Configuration...
   3. Console Passwords...
   4. Event Log
   5. Command Line (CLI)
   6. Reboot Switch
   7. Download OS
   8. Run Setup
   0. Logout


Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

mesh

OVERVIEW

Category:	Redundant Paths
Primary context:	config
Related Commands	**show mesh (page 488)**

```
Usage: [no] mesh [ethernet] PORT-LIST

Description: Configure the specified ports as being members of a mesh group.
             A mesh group can have up to 24 member ports.

           - VLAN support must be enabled before configuring a mesh group.
           - A mesh group cannot exist if IP routing is enabled.  Disable
             routing protocols (if any) before configuring a mesh group.
           - After configuring meshing, it will be necessary to reboot the
             switch before the changes take effect.
```

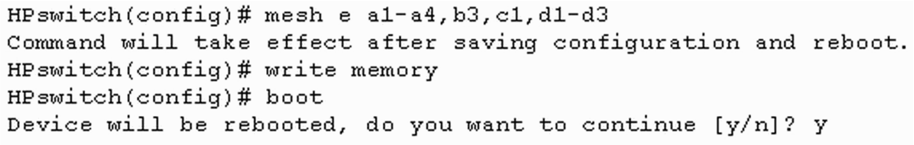
COMMAND STRUCTURE

- [no] mesh **portlist** -- Specify the ports that are to be added to/removed from a mesh. ([ethernet] PORT-LIST) **(p. 352)**

EXAMPLES

Example: mesh PORT-LIST

Configure meshing on ports A1-A4, B3, C1, and D1-D3:



```
HPswitch(config)# mesh e a1-a4,b3,c1,d1-d3
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

COMMAND DETAILS

portlist (p. 352)

portlist

- [no] mesh *[ETHERNET] PORT-LIST*

```
Specify the ports that are to be added to/removed from a mesh.
```

mirror

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: 1) mirror <1-4> [ name NAME-STR ] port PORT-NUM
       2) mirror <1-4> [ name NAME-STR ] remote ip SRC-IP-ADDR
                       SRC-UDP-PORT DST-IP-ADDR
       3) mirror <1-4> [ name NAME-STR ] remote ip SRC-IP-ADDR
                       SRC-UDP-PORT DST-IP-ADDR
       4) no mirror <1-4> [ name NAME-STR ]
       5) mirror endpoint ip SRC-IP-ADDR SRC-UDP-PORT DST-IP-ADDR
                        port PORT-NUM
       6) no mirror endpoint ip SRC-IP-ADDR SRC-UDP-PORT DST-IP-ADDR

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  o <1-4> - Mirror destination number
             o name NAME-STR - Friendly name to be associated with the
             mirror destionation number.
             o PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
             o SRC-IP-ADDR - source ip address for remote mirroring.
             o SRC-UDP-PORT - source UDP port for remote mirroring.
             o DST-IP-ADDR - destination ip address for remote mirroring.

Note1: The SRC-IP-ADDR, SRC-UDP-PORT, and DST-IP-ADDR specified on the
       source switch must match those on the respective destination switch.
Note2: The SRC-IP-ADDR, SRC-UDP-PORT, and DST-IP-ADDR must not be uses if the
       'no' keyword is used unless the 'endpoint' keyword is used.
```

COMMAND STRUCTURE

- [no] mirror **endpoint** -- Remote mirroring destination configuration. **(p. 354)**
  - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 354)**
    - **mirror_session_ip_udp** **< 1 to 65535 >** -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 355)**
      - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 355)**
        - **port** -- Remote mirroring destination port. ([ethernet] PORT-NUM) **(p. 356)**
- [no] mirror **mirror_session_id** **< 1 to 4 >** -- Mirror destination number. **(p. 355)**
  - **name** -- Mirroring destination name string. (ASCII-STR) **(p. 356)**
    - **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 356)**

    - **remote** -- Remote mirroring destination configuration. **(p. 356)**
      - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 354)**
        - **mirror_session_src_udp < 1 to 65535 >** -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 355)**
          - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 355)**
  - **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 356)**
  - **remote** -- Remote mirroring destination configuration. **(p. 356)**
    - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 354)**
      - **mirror_session_src_udp < 1 to 65535 >** -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 355)**
        - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 355)**
- [no] mirror **name** -- Mirror destination name. **(p. 356)**

COMMAND DETAILS

endpoint (p. 354)
ip (p. 354)
mirror_session_dest_ip (p. 355)
mirror_session_id (p. 355)
mirror_session_ip_udp (p. 355)
mirror_session_src_udp (p. 355)
name (p. 356)
port (p. 356)
remote (p. 356)

endpoint

- [no] mirror endpoint

```
Remote mirroring destination configuration.
```

Next Available Option:

- **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 354)**

ip

- mirror *< 1 to 4 >* name *NAME* remote ip *IP-ADDR*

```
Remote mirroring destination configuration.
```

Next Available Option:

- **mirror_session_src_udp** < 1 to 65535 > -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 355)**

- mirror *< 1 to 4 >* remote ip *IP-ADDR*

```
Remote mirroring destination configuration.
```

Next Available Option:

- **mirror_session_src_udp** < 1 to 65535 > -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 355)**

- [no] mirror endpoint ip *IP-ADDR*

```
Remote mirroring destination configuration.
```

Next Available Option:

- **mirror_session_ip_udp** < 1 to 65535 > -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 355)**

mirror_session_dest_ip

- mirror *< 1 to 4 >* name *NAME* remote ip *IP-ADDR < 1 to 65535 > IP-ADDR*

  `Remote mirroring UDP encapsulation destination ip addr.`

- mirror *< 1 to 4 >* remote ip *IP-ADDR < 1 to 65535 > IP-ADDR*

  `Remote mirroring UDP encapsulation destination ip addr.`

- [no] mirror endpoint ip *IP-ADDR < 1 to 65535 > IP-ADDR*

  `Remote mirroring UDP encapsulation destination ip addr.`

Next Available Option:

- **port** -- Remote mirroring destination port. ([ethernet] PORT-NUM) **(p. 356)**

mirror_session_id

- [no] mirror *< 1 to 4 >*

  `Mirror destination number.`

Range: < 1 to 4 >

Next Available Options:

- **name** -- Mirroring destination name string. (ASCII-STR) **(p. 356)**
- **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 356)**
- **remote** -- Remote mirroring destination configuration.**(p. 356)**

mirror_session_ip_udp

- [no] mirror endpoint ip *IP-ADDR < 1 to 65535 >*

  `Remote mirroring UDP encapsulation port.`

Range: < 1 to 65535 >

Next Available Option:

- **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 355)**

mirror_session_src_udp

- mirror *< 1 to 4 >* name *NAME* remote ip *IP-ADDR < 1 to 65535 >*

  `Remote mirroring UDP encapsulation port.`

Range: < 1 to 65535 >

Next Available Option:

- **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 355)**

- mirror *< 1 to 4 >* remote ip *IP-ADDR* *< 1 to 65535 >*

  ```
  Remote mirroring UDP encapsulation port.
  ```

  Range: < 1 to 65535 >

  Next Available Option:

  - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 355)**

name

- mirror *< 1 to 4 >* name *NAME*

  ```
  Mirroring destination name string.
  ```

  Next Available Options:

  - **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 356)**
  - **remote** -- Remote mirroring destination configuration.**(p. 356)**

- [no] mirror name

  ```
  Mirror destination name.
  ```

port

- mirror *< 1 to 4 >* name *NAME* port *[ETHERNET] PORT-NUM*

  ```
  Mirroring destination monitoring port.
  ```

- mirror *< 1 to 4 >* port *[ETHERNET] PORT-NUM*

  ```
  Mirroring destination monitoring port.
  ```

- mirror endpoint ip *IP-ADDR* *< 1 to 65535 >* *IP-ADDR* port *[ETHERNET] PORT-NUM*

  ```
  Remote mirroring destination port.
  ```

remote

- mirror *< 1 to 4 >* name *NAME* remote

  ```
  Remote mirroring destination configuration.
  ```

  Next Available Option:

  - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 354)**

- mirror *< 1 to 4 >* remote

  ```
  Remote mirroring destination configuration.
  ```

Next Available Option:

- **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 354)**

mirror-port

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**vlan (page 611)**

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

COMMAND STRUCTURE

- [no] mirror-port **port_num** -- Define the mirror port for diagnostic purposes ([ethernet] PORT-NUM) **(p. 358)**

EXAMPLES

Example: mirror-port

Assign port A6 as the monitoring port:

```
ProCurve(config)# mirror-port a6
```

COMMAND DETAILS

port_num (p. 358)

port_num

- [no] mirror-port *[ETHERNET] PORT-NUM*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
```

```
cannot be a trunked port. The parameter must be specified,
if the 'no' keyword is not used. Otherwise, it must not be
present.
```

module

OVERVIEW

Category:	config
Primary context:	config
Related Commands	show modules (page 489)

```
Usage: module <MODULE-NUM>  module-type <MODULE-TYPE>
```

```
Description: Configure type of the module.
```

COMMAND STRUCTURE

- module < 1 to 12 > type **< J8701A | J8702A | J8705A | ... >** -- The type of the module. (p. 360)

EXAMPLES

Example: module SLOT-NUM type MODULE-TYPE

Configure slot 4 for module type j4820a:

```
ProCurve(config)# module 4 type j4820a
```

COMMAND DETAILS

type (p. 360)

type

- module *< 1 to 12 >* type *< J8701A | J8702A | J8705A | ... >*

  ```
  The type of the module.
  ```

  Supported Values:

  - **J8701A**
  - **J8702A**
  - **J8705A**
  - **J8706A**
  - **J8707A**
  - **J8708A**
  - **J86yyA**
  - **J86xxA**
  - **J86yyA**
  - **J86xxA**
  - **J8694A**
  - **J8992A**
  - **J90XXA**
  - **JXXXXA**
  - **JXXXXB**
  - **JXXXXA**
  - **J9051A**
  - **J9052A**

monitor

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show monitor (page 489)**

```
Usage: [no] monitor mac MAC-ADDR <src | dst | both> mirror <1-4 | NAME-STR>

Description: Set up traffic monitoring for a given MAC address. Network
             traffic with this MAC address as the source or destination is
             copied to the mirror port.

Parameters:  o MAC-ADDR - MAC address to be monitored
             o <src | dst | both> - Type of traffic to monitor:
             src - Monitor traffic with MAC-ADDR as the source.
             dst - Monitor traffic with MAC-ADDR as the destination.
             both - Monitor traffic with MAC-ADDR as the source or
             destination.
             o <1-4> - Mirror destination number
             o NAME-STR - Friendly name associated with the mirror
             destionation number.
```

COMMAND STRUCTURE

- [no] monitor **mac** -- MAC address. (MAC-ADDR) **(p. 361)**
  - **monitor_mac_direction < src | dst | both >** -- **(p. 362)**
    - **mirror** -- Mirror destination. **(p. 361)**
      - **mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 362)**
      - **mirror_session_name** -- Mirror destination name. **(p. 362)**

COMMAND DETAILS

mac (p. 361)
mirror (p. 361)
mirror_session_id (p. 362)
mirror_session_name (p. 362)
monitor_mac_direction (p. 362)

mac

- [no] monitor mac *MAC-ADDR*

```
Configures the MAC address as selection criteria for mirroring traffic on
any port or learned VLAN on the switch.
```

Next Available Option:

- **monitor_mac_direction** < src | dst | both > -- **(p. 362)**

mirror

- [no] monitor mac *MAC-ADDR* < *src* | *dst* | *both* > mirror

```
Mirror destination. Assigns the inbound and/or outbound traffic filtered by the
specified
MAC address to a previously configured mirroring session. The session is identified
by a
```

```
number or (if configured) a name.
Depending on how many sessions are configured on the switch, you can use the same
command
to configure a MAC address as mirroring criteria in up to four sessions. To identify
 a
session, you can enter either its name or number; for example: mirror 1 2 3 traffsrc4
```

Next Available Options:

- **mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 362)**
- **mirror_session_name** -- Mirror destination name.**(p. 362)**

mirror_session_id

- [no] monitor mac *MAC-ADDR* < *src* | *dst* | *both* > mirror < *1 to 4* >

```
Mirror destination number.
```

Range: < 1 to 4 >

mirror_session_name

- [no] monitor mac *MAC-ADDR* < *src* | *dst* | *both* > mirror

```
Mirror destination name.
```

monitor_mac_direction

- [no] monitor mac *MAC-ADDR* < *src* | *dst* | *both* >

```
Specifies how the MAC address is used to filter and mirror packets in inbound and/or
 outbound
traffic on the interfaces on which the mirroring session is applied.
```

Supported Values:

- **src** -- Monitor traffic with this MAC as source
- **dst** -- Monitor traffic with this MAC as destination
- **both** -- Monitor traffic with this MAC as source or destination

Next Available Option:

- **mirror** -- Mirror destination.**(p. 361)**

page

OVERVIEW

Category:	CLI Setup
Primary context:	manager
Related Commands	

```
Usage: [no] page

Description: Toggle paging mode. The printing is paused when a full page
             of text has been displayed, or continues until end of output.
```

COMMAND STRUCTURE

password

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**front-panel-security (page 177)** **show front-panel-security (page 473)**

```
Usage: [no] password <manager|operator|port-access|all>
                        [user-name ASCII-STR] [<plaintext|sha1> ASCII-STR]

Description: Set or clear local password/username for a given access level.
             Invoked without 'no', the command sets or changes existent
             password(s). If no password provided in the command, the user
             will be prompted to enter the new password twice. The command
             removes specific local password protection, if preceded by 'no'.
Parameters:
    o <manager|operator|port-access|all> - Level of access.
    o user-name ASCII-STR - Username (up to 16 characters).
    o <plaintext|sha-1> ASCII-STR - Format for the password entry, and
             the password itself (up to 16 characters). 'plaintext' is
             default type, and the only type accepted for 'port-access'.
```

COMMAND STRUCTURE

- [no] password **access < operator | manager | port-access >** -- Set or clear local password/username for a given access level **(p. 365)**
  - **hashtype < plaintext | sha-1 >** -- Set hash type. **(p. 365)**
    - **password** -- Set password (ASCII-STR) **(p. 366)**
  - **user-name** -- Set username for the specified user category. (ASCII-STR) **(p. 366)**
    - **hashtype < plaintext | sha-1 >** -- Set hash type. **(p. 365)**
      - **password** -- Set password (ASCII-STR) **(p. 366)**
- [no] password **all < all >** -- Set or clear local password/username for a given access level **(p. 365)**

EXAMPLES

Example: password

Configure manager and operator passwords:

ProCurve(config) # password manager

New password: ********

Please retype new password: ********

ProCurve(config)# password operator

New password: ********

Please retype new password: ********

COMMAND DETAILS

access

- [no] password *< operator | manager | port-access >*

```
Usage: [no] password <manager|operator|port-access|all>
                          [user-name ASCII-STR] [<plaintext|sha1> ASCII-STR]

Description: Set or clear local password/username for a given access level.
             Invoked without 'no', the command sets or changes existent
             password(s). If no password provided in the command, the user
             will be prompted to enter the new password twice. The command
             removes specific local password protection, if preceded by 'no'.
Parameters:
    o <manager|operator|port-access|all> - Level of access.
    o user-name ASCII-STR - Username (up to 16 characters).
    o <plaintext|sha-1> ASCII-STR - Format for the password entry, and
             the password itself (up to 16 characters). 'plaintext' is
             default type, and the only type accepted for 'port-access'.
```

Supported Values:

- **operator** -- Configure operator access.
- **manager** -- Configure manager access.
- **port-access** -- Configure port access.

Next Available Options:

- **user-name** -- Set username for the specified user category. (ASCII-STR) **(p. 366)**
- **hashtype** < plaintext | sha-1 > -- Set hash type.**(p. 365)**

all

- [no] password *< all >*

```
Usage: [no] password <manager|operator|port-access|all>
                          [user-name ASCII-STR] [<plaintext|sha1> ASCII-STR]

Description: Set or clear local password/username for a given access level.
             Invoked without 'no', the command sets or changes existent
             password(s). If no password provided in the command, the user
             will be prompted to enter the new password twice. The command
             removes specific local password protection, if preceded by 'no'.
Parameters:
    o <manager|operator|port-access|all> - Level of access.
    o user-name ASCII-STR - Username (up to 16 characters).
    o <plaintext|sha-1> ASCII-STR - Format for the password entry, and
             the password itself (up to 16 characters). 'plaintext' is
             default type, and the only type accepted for 'port-access'.
```

Supported Values:

- **all** -- Configure all available types of access.

hashtype

- password *< operator | manager | port-access >* user-name *USER-NAME < plaintext |*

sha-1 >

```
Specifies the type of algorithm (if any) used to hash the password. Valid
values are plaintext or sha-1.
Note: You can enter a manager, operator, or 802.1X port-access password in
clear ASCII text or hashed format. However, manager and operator passwords
are displayed and saved in a configuration file only in hashed format;
port-access passwords are displayed and saved only as plain ASCII text.
```

Supported Values:

- **plaintext** -- Enter plaintext password.
- **sha-1** -- Enter SHA-1 hash of password.

Next Available Option:

- **password** -- Set password (ASCII-STR) **(p. 366)**

- password *< operator | manager | port-access > < plaintext | sha-1 >*

```
The clear ASCII text string or SHA-1 hash of the password.
```

Supported Values:

- **plaintext** -- Enter plaintext password.
- **sha-1** -- Enter SHA-1 hash of password.

Next Available Option:

- **password** -- Set password (ASCII-STR) **(p. 366)**

password

- password *< operator | manager | port-access >* user-name *USER-NAME < plaintext | sha-1 > PASSWORD*

```
Set password
```

- password *< operator | manager | port-access > < plaintext | sha-1 > PASSWORD*

```
Set password
```

user-name

- password *< operator | manager | port-access >* user-name *USER-NAME*

```
Set username for the specified user category.
```

Next Available Option:

- **hashtype** < plaintext | sha-1 > -- Set hash type.**(p. 365)**

ping

OVERVIEW

Category:	
Primary context:	operator
Related Commands	**traceroute (page 598)** **link-test (page 327)** **ping6 (page 369)**

```
Usage: ping <IP-ADDR|hostname|SWITCH-NUM>
            [repetitions <1-10000>] [timeout <1-60>]
            [data-size <0-65471>] [data-fill <0-1024>]

Description: Send IPv4 ping request(s) to a device on the network.

Parameters:

   o IP-ADDR - IPv4 address of device to ping.

   o hostname - Hostname of device to which to send IPv4 ping.

   o [repetitions <1-10000>] - Number of times to send ping; the default
     value is 1.

   o [timeout <1-60>] - Seconds within which a response is required
     before the test is considered as failed; the default value is 5.

   o [data-size <0-65471>] - Size of data to send; the default
     size is 0.

   o [data-fill <0-1024>] - The string to be filled in the data portion
     of the packet. A string upto 1024 characters in length can be
     specified. The default value is a 0 length string.

Examples:

    (1) hp-switch# ping 1.1.1.1
```

COMMAND STRUCTURE

- ping **data-fill** -- Ping data fill string (size <0-1024>). (OCTET-STR) **(p. 368)**
- ping **data-size** **< 0 to 65471 >** -- Ping data size <0-65471>. (NUMBER) **(p. 368)**
- ping **host-name** -- Hostname of the device to ping. (ASCII-STR) **(p. 368)**
- ping **ip-addr** -- IPv4 address of the device to ping. (IP-ADDR) **(p. 368)**
- ping **repetitions** **< 1 to 10000 >** -- Number of packets to send <1-10000>. (NUMBER) **(p. 368)**
- ping **switch-num** -- The stack number of the switch to ping. (NUMBER) **(p. 368)**
- ping **timeout** **< 1 to 60 >** -- Ping timeout in seconds <1-60>. (NUMBER) **(p. 368)**

EXAMPLES

Example: ping IP-ADDR

Send an IP Ping request to the device that has IP address 10.10.10.1:

```
ProCurve# ping 10.10.10.1
10.10.10.1 is alive, time = 50 ms
```

COMMAND DETAILS

data-fill

- ping data-fill *OCTET-STR*

  `Ping data fill string (size <0-1024>).`

data-size

- ping data-size *< 0 to 65471 >*

  `Ping data size <0-65471>.`

  Range: < 0 to 65471 >

host-name

- ping *HOST-NAME*

  `Hostname of the device to ping.`

ip-addr

- ping *IP-ADDR*

  `IPv4 address of the device to ping.`

repetitions

- ping repetitions *< 1 to 10000 >*

  `Number of packets to send <1-10000>.`

  Range: < 1 to 10000 >

switch-num

- ping *NUMBER*

  `The stack number of the switch to ping.`

timeout

- ping timeout *< 1 to 60 >*

  `Ping timeout in seconds <1-60>.`

  Range: < 1 to 60 >

ping6

OVERVIEW

Category:	
Primary context:	operator
Related Commands	**ping (page 367)** **traceroute6 (page 601)**

```
Usage: ping6 <IPV6-ADDR|hostname>
            [repetitions <1-10000>] [timeout <1-60>]
            [data-size <0-65471>] [data-fill <0-1024>]

Description: Send IPv6 ping request(s) to a device on the network.

Parameters:

   o IPV6-ADDR - IPv6 address of device to ping.

   o hostname   - Hostname of device to which to send IPv6 ping.

   o [repetitions <1-10000>] - Number of times to send ping; the default
     value is 1.

   o [timeout <1-60>] - Seconds within which a response is required
     before the test is considered as failed; the default value is 5.

   o [data-size <0-65471>] - Specifies the size of the data in the ICMP echo
      packet; the default value is 0.
   o [data-fill <1-10000>] - Specifies the data pattern to be filled in the
      data of the ICMP echo packet; the default pattern is .
Examples:

    (1) ProCurve# ping6 80fe::20b:cdff:fedd:9a62
    (2) ProCurve# ping6 fe80::5%vlan20
```

COMMAND STRUCTURE

- ping6 **data-fill** -- Ping data fill string (size <0-1024>). (OCTET-STR) **(p. 369)**
- ping6 **data-size < 0 to 65471 >** -- Ping data size <0-65471>. (NUMBER) **(p. 370)**
- ping6 **host-name** -- Hostname of the device to ping. (ASCII-STR) **(p. 370)**
- ping6 **ipv6-addr** -- IPv6 address of device to ping. (IPV6-ADDR) **(p. 370)**
- ping6 **repetitions < 1 to 10000 >** -- Number of packets to send <1-10000>. (NUMBER) **(p. 370)**
- ping6 **timeout < 1 to 60 >** -- Ping timeout in seconds <1-60>. (NUMBER) **(p. 370)**

COMMAND DETAILS

data-fill (p. 369)	**host-name (p. 370)**	**repetitions (p. 370)**
data-size (p. 370)	**ipv6-addr (p. 370)**	**timeout (p. 370)**

data-fill

- ping6 data-fill *OCTET-STR*

```
Text string used as data in ping packets. You can enter up to 1024
alphanumeric characters in the text.
Valid values: 0-1024.
```

Default: 0 (no text is used)

data-size

- ping6 data-size *< 0 to 65471 >*

```
Size of data (in bytes) to be ent in ping packets.
Valid values: 0-65471.
```

Range: < 0 to 65471 >

Default: 0

host-name

- ping6 *HOST-NAME*

```
Hostname of the device to ping.
```

ipv6-addr

- ping6 *IPV6-ADDR*

```
IPv6 address of device to ping.
```

repetitions

- ping6 repetitions *< 1 to 10000 >*

```
Number of times that IPv6 ping packets are sent to the destination
IPv6 host. Valid values are: <1-10000>.
```

Range: < 1 to 10000 >

Default: 1

timeout

- ping6 timeout *< 1 to 60 >*

```
Number of seconds within which a response is required from the destination
host before the ping test times out. Valid values: <1-60>.
```

Range: < 1 to 60 >

Default: 1 second

port-security

OVERVIEW

Category:	Port Security
Primary context:	config
Related Commands	**show port-security (page 498)** **show mac-address (page 487)**

```
Usage: [no] port-security [ethernet] PORT-LIST
          [learn-mode <continuous|static|configured|
                       limited-continuous|port-access>]
          [address-limit <1-32>]
          [mac-address MAC-ADDR [MAC-ADDR ...]]
          [action <none|send-alarm|send-disable>]
          [clear-intrusion-flag]

Description: Set the port-security operation(s) for each port in port list.

Parameters:

    o learn-mode <continuous|static|configured|limited-continuous|port-access>
             If 'continuous' is specified, the port continually learns new
             addresses on the port. If 'static' is specified, the user
             can configure addresses that are authorized to use on that port
             and let the switch learn the remaining addresses up to the
             specified address-limit. If 'configured' is specified, up
             to address-limit configured addresses are authorized. Use the
             'address-limit' parameter to specify the maximum number of
             static addresses for the port.
             The 'port-access' instructs the device to learn only the MAC
             addresses authorized by 802.1X or Web/MAC authentication
             subsystem. After a MAC address is authorized, only traffic
             from the authorized MAC address is allowed.
             If 'limited-continuous' is specified, the first
             'address-limit' source MAC addresses heard on this
             port become the authorized addresses. When new authorized
             addresses are learned, they are stored in a table. When
             the table has reached its 'address-limit', any
             new source MAC addresses received on the port
             constitutes an intrusion. The authorized addresses in
             this mode will age out of the system, therefore the
             list of authorized addresses can be dynamic over time.
    o address-limit <1-N> - This parameter is valid only when the learn-mode
             is static, configured, or limited-continuous.
             It defines the number of MAC address that the table for the
             given port will hold. For static and configured N is equal
             to 8. For limited-continuous N is equal to 32.
    o mac-address MAC-ADDR ... - This 12-hex digit parameter is only valid
             when the learn-mode is static. The parameter is used to configure
             the addresses that are authorized to use the port. The maximum
             number of authorized addresses that may be configured and
             learned is 8. If the number of configured addresses is less
             than the address-limit, the switch will learn the remaining
             number of addresses. Several addresses can be specified in
             one command line.
```

```
o action <none|send-alarm|send-disable> - Indicates the port security
         action the switch will take if an intruder is detected on the
         port.
o clear-intrusion-flag - clears intrusion indicator for the ports
         specified in the command PORT-LIST.
```

COMMAND STRUCTURE

- port-security [ETHERNET] PORT-LIST **action < none | send-alarm | send-disable >** -- Define device's action in case of an intrusion detection. **(p. 372)**
- port-security [ETHERNET] PORT-LIST **address-limit < 1 to 32 >** -- Define number of authorized addresses on the port(s). **(p. 373)**
- port-security [ETHERNET] PORT-LIST **clear-intrusion-flag** -- Clear intrusion indicator for the port(s) **(p. 373)**
- port-security [ETHERNET] PORT-LIST **learn-mode < continuous | static | configured | ... >** -- Define the mode of acquiring authorized MAC address(es). **(p. 373)**
- [no] port-security [ETHERNET] PORT-LIST **mac-address** -- Configure the address(es) authorized on the port(s). **(p. 373)**
  - **mac-addr** -- Authorized MAC address. (MAC-ADDR) **(p. 373)**

EXAMPLES

Example: port-security learn-mode

Configure port A1 to automatically accept the first device (MAC address) it detects as the only authorized device for that port. (The default device limit is 1.) This command also configures the port to send an alarm to a network management station and disable itself if an intruder is detected on the port.

```
ProCurve(config)# port-security a1 learn-mode static action send-disable
```

Example: port-security learn-mode

Configure port A5 to allow two MAC addresses, 00c100-7fec00 and 0060b0-889e00, as the authorized devices. This command also configures the switch to send an alarm to a management station if an intruder is detected on the port, but nonetheless to allow the intruder to access to the network.

```
ProCurve(config)# port-security a5 learn-mode static
address-limit 2 mac-address 00c100-7fec00 0060b0-889e00
action send-alarm
```

COMMAND DETAILS

action (p. 372)	**clear-intrusion-flag (p. 373)**	**mac-addr (p. 373)**
address-limit (p. 373)	**learn-mode (p. 373)**	**mac-address (p. 373)**

action

- port-security *[ETHERNET] PORT-LIST* action *< none | send-alarm | send-disable >*

  ```
  Define device's action in case of an intrusion detection.
  ```

  Supported Values:
  - **none**
  - **send-alarm**
  - **send-disable**

address-limit

- port-security *[ETHERNET] PORT-LIST* address-limit *< 1 to 32 >*

  ```
  Define number of authorized addresses on the port(s).
  ```

  Range: < 1 to 32 >

clear-intrusion-flag

- port-security *[ETHERNET] PORT-LIST* clear-intrusion-flag

  ```
  Clear intrusion indicator for the port(s)
  ```

learn-mode

- port-security *[ETHERNET] PORT-LIST* learn-mode *< continuous | static | configured | ... >*

  ```
  Define the mode of acquiring authorized MAC address(es).
  ```

  Supported Values:

  - **continuous** -- Continuous MAC address learn mode.
  - **static** -- Static MAC address learn mode.
  - **configured** -- Static MAC address configured mode.
  - **port-access** -- Learn port-access authorized MAC address only.
  - **limited-continuous** -- Limited continuous MAC address learn mode.

mac-addr

- port-security *[ETHERNET] PORT-LIST* mac-address *MAC-ADDR*

  ```
  Authorized MAC address.
  ```

mac-address

- [no] port-security *[ETHERNET] PORT-LIST* mac-address

  ```
  Configure the address(es) authorized on the port(s).
  ```

  Next Available Option:

  - **mac-addr** -- Authorized MAC address. (MAC-ADDR) **(p. 373)**

power-over-ethernet

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show power-over-ethernet (page 499)**

```
Usage: power [slot <SLOT-LIST>] [threshold <1-99>][optional-parameters]

Description: Set Power Over Ethernet(poe) configuration parameters.
             threshold - set the power consumption percentage at which
                         a trap should be sent.
             optional-parameters - Use <TAB> or <?> after entering power
                         to see a list of all available options.
```

NOTES

Replaces "power" Command

The "interface power-over-ethernet" command replaces the " interface power" command that was used in earlier versions. The "show power-over-ethernet" command replaces the "show power-management" command that was used in earlier versions.

COMMAND STRUCTURE

- [no] power-over-ethernet **pre-std-detect** -- Detect and power pre-802.3af **(p. 374)**
- [no] power-over-ethernet **redundancy** -- Set how much power is held in reserve for redundancy **(p. 374)**
  - **redundancy_type < n+1 | full >** -- Set how much power is held in reserve for redundancy (NUMBER) **(p. 375)**
- power-over-ethernet **slot** -- Optional - Specify a valid powered-slot list for power threshold setting or omit to set all powered-slots. (SLOT-ID-RANGE) **(p. 375)**
  - **threshold < 1 to 99 >** -- Set the power consumption percentage at which a trap should be sent. (NUMBER) **(p. 375)**
- power-over-ethernet **threshold < 1 to 99 >** -- Set the power consumption percentage at which a trap should be sent. (NUMBER) **(p. 375)**

COMMAND DETAILS

pre-std-detect (p. 374)
redundancy (p. 374)
redundancy_type (p. 375)
slot (p. 375)
threshold (p. 375)

pre-std-detect

- [no] power-over-ethernet pre-std-detect

```
Usage: [NO] power-over-ethernet pre-std-detect

Description: Detect and power pre-802.3af-standard devices. This is enabled
by default.
```

redundancy

- [no] power-over-ethernet redundancy

```
Usage: [NO] power redundancy [n+1|full]

Description: Set how much power is held in reserve for redundancy.
             NO   - All available power can be allocated to powered devices.
             n+1  - One of the highest power supplies will be held in
                    reserve. In the event of a simgle power supply failure,
                    no powered devices will be shut down.
             full - Half of the available power supplies will be held in
                    reserve.

             Default: No PoE redundancy enforced.
```

Next Available Option:

- **redundancy_type** < n+1 | full > -- Set how much power is held in reserve for redundancy (NUMBER) **(p. 375)**

redundancy_type

- power-over-ethernet redundancy *< n+1 | full >*

```
Usage: [NO] power redundancy [n+1|full]

Description: Set how much power is held in reserve for redundancy.
             NO   - All available power c11111111111111111111111111111111111111`an
be allocated to powered devices.
             n+1  - One of the highest power supplies will be held in
                    reserve. In the event of a simgle power supply failure,
                    no powered devices will be shut down.
             full - Half of the available power supplies will be held in
                    reserve.
```

Supported Values:

- **n+1**
- **full**

slot

- power-over-ethernet slot *SLOT-ID-RANGE*

```
Optional - Specify a valid powered-slot list for power threshold setting or
           omit to set all powered-slots.
```

Next Available Option:

- **threshold** < 1 to 99 > -- Set the power consumption percentage at which a trap should be sent. (NUMBER) **(p. 375)**

threshold

- power-over-ethernet threshold *< 1 to 99 >*

```
Set the power consumption percentage at which a trap should be sent.

Note that the last "threshold" command affecting a given slot supersedes
the previous threshold command affecting the same slot.
```

Range: < 1 to 99 >

- power-over-ethernet slot *SLOT-ID-RANGE* threshold *< 1 to 99 >*

  ```
  Set the power consumption percentage at which a trap should be sent.
  ```

  Range: < 1 to 99 >

primary-vlan

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show vlan (page 518)**

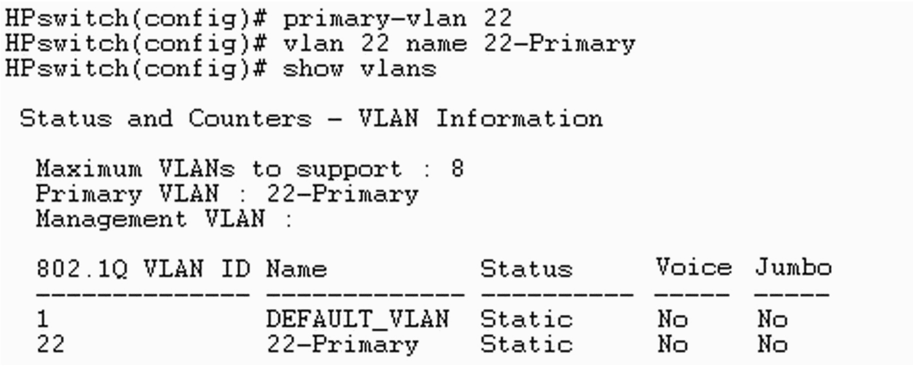
```
Usage: primary-vlan VLAN-ID

Description: Set the VLAN that is to be used as the primary VLAN.
             The primary VLAN comes into play for features such as
             stacking, DHCP, and TIMEP.
```

COMMAND STRUCTURE

EXAMPLES

Example: primary-vlan VLAN-ID

Reassign the Primary VLAN and change the VLAN name:



```
HPswitch(config)# primary-vlan 22
HPswitch(config)# vlan 22 name 22-Primary
HPswitch(config)# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : 22-Primary
  Management VLAN :

  802.1Q VLAN ID Name           Status     Voice  Jumbo
  -------------- -------------- ---------- -----  -----
  1              DEFAULT_VLAN   Static     No     No
  22             22-Primary     Static     No     No
```

print

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: print COMMAND-STR

Description: Execute a command and redirect its output to the device channel
             for current session.
```

COMMAND STRUCTURE

- print **command** -- Command to execute. Use quotes for multiword commands. (ASCII-STR) **(p. 378)**

COMMAND DETAILS

command (p. 378)

command

- print *COMMAND*

  ```
  Command to execute. Use quotes for multiword commands.
  ```

p-wireless-services

OVERVIEW

Category:	
Primary context:	config
Related Commands	

COMMAND STRUCTURE

- p-wireless-services **p-wireless-services** -- (SLOT-ID) **(p. 379)**
  - **config** -- (ASCII-STR) **(p. 379)**

COMMAND DETAILS

config (p. 379)	**p-wireless-services (p. 379)**

config

- p-wireless-services *SLOT-ID* config *CONFIG*

p-wireless-services

- p-wireless-services *SLOT-ID*

  Next Available Option:
  - **config** -- (ASCII-STR) **(p. 379)**

qinq

OVERVIEW

Category:	
Primary context:	config
Related Commands	svlan (page 572) vlan (page 611) show qinq (page 500)

```
Usage:  [no] qinq [ <mixedvlan|svlan> [tag-type<tpid>] ]

Description: Configure the device qinq mode. The command 'no qinq' disables
             qinq on the device (no tag-stacking). Changing qinq mode from
             one to another requires reboot to take effect and the device
             will boot up with a default configuration for the new qinq mode.

Parameters:
   mixedvlan - This is a qinq mode with support for both CVLANs and SVLANs.
   svlan     - This is a qinq mode with only SVLANs support.
   tag-type  - The tpid (ethertype) for provider tagged frames. The default
               tpid value is 0x88a8.
```

COMMAND STRUCTURE

- qinq **mixedvlan** -- Configure as mixedvlan mode **(p. 380)**
  - **tag-type < 1536 to 65535 >** -- Configure qinq tag-type (HEX NUMBER) **(p. 381)**
- qinq **svlan** -- Configure as svlan mode **(p. 380)**
  - **tag-type < 1536 to 65535 >** -- Configure qinq tag-type (HEX NUMBER) **(p. 381)**

COMMAND DETAILS

mixedvlan (p. 380)	**svlan (p. 380)**	**tag-type (p. 381)**

mixedvlan

- qinq mixedvlan

```
Configure as mixedvlan mode. Mixed vlan mode configuration supports both C-VLAN
and S-VLAN operations on the same device. This allows the use of S-VLAN member
ports for QinQ tunneling.
The main advantage for mixed vlan mode is that users do not have to dedicate
the entire switch as a QinQ access switch.
Requires a reboot to take effect.
```

Next Available Option:

- **tag-type** < 1536 to 65535 > -- Configure qinq tag-type (HEX NUMBER) **(p. 381)**

svlan

- qinq svlan

```
Configure as svlan mode. Globally enables QinQ svlan mode, an S-VLAN only
environment that supports port-based or s-tagged interfaces of the standard.
Requires a reboot to take effect.
```

Next Available Option:

- **tag-type** < 1536 to 65535 > -- Configure qinq tag-type (HEX NUMBER) **(p. 381)**

tag-type

- qinq mixedvlan tag-type *< 1536 to 65535 >*

  ```
  Configure qinq tag-type
  ```

  Range: < 1536 to 65535 >
- qinq svlan tag-type *< 1536 to 65535 >*

  ```
  Configure qinq tag-type
  ```

  Range: < 1536 to 65535 >

qos

OVERVIEW

Category:	QoS
Primary context:	config
Related Commands	**show qos (page 500)**

```
Usage: [no] qos ...

Description: Configure Quality of Service (QoS) on the device. The
             command must be followed by a keyword defining a subdomain
             of the QoS parameters to configure.
```

COMMAND STRUCTURE

- [no] qos **apptype < udp-port | tcp-port >** -- Configure priorities for TCP/UDP services **(p. 383)**
  - **port-num** -- TCP/UDP port from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 388)**
    - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 386)**
    - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 388)**
  - **range** -- Specify range of TCP/UDP ports from [to] which to prioritize traffic. **(p. 391)**
    - **port-num** -- TCP/UDP port from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 388)**
      - **max-port-num** -- Maximal TCP/UDP port in the range from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 388)**
        - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 386)**
        - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 388)**
- [no] qos **device-priority** -- Configure device-based priority (IP-ADDR) **(p. 385)**
  - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 386)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 388)**
- [no] qos **dscp-map < 000000 | 000001 | 000010 | ... >** -- Define mapping between a DSCP (Differentiated-Services Codepoint) value and an 802.1p priority. **(p. 386)**
  - **name** -- Specify DSCP->priority mapping name. **(p. 388)**
    - **name-string** -- Specify DSCP->priority mapping name. (ASCII-STR) **(p. 388)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 388)**
- [no] qos **protocol < IP | IPX | ARP | ... >** -- Configure protocol-based priority **(p. 390)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 388)**
- qos **queue-config** -- Sets the number of outbound port queues that buffer the packets depending on their 802.1p priority. **(p. 390)**
  - **2-queues** -- Set the number of outbound port queues for all switch ports. **(p. 383)**
  - **4-queues** -- Set the number of outbound port queues for all switch ports. **(p. 383)**
  - **8-queues** -- Set the number of outbound port queues for all switch ports. **(p. 383)**
- [no] qos **type-of-service** -- Configure the Type-of-Service method the device uses to prioritize IP traffic **(p. 391)**
  - **diff-services** -- In IP Differentiated Services (Diffserv) mode, IPv4 packets are classified and given a QoS priority based on the upper 6 bits of the IP ToS field from the packets as they enter the switch. The assignment of Diffserv Codepoints to 802.1p priorities is done via the qos dscp-map command. Any Diffserv Codepoint in an inbound IPv4 packet can be re-mapped to a different codepoint (and its associated 802.1p priority) on outbound. This is done by using the syntax: qos type-of-service diff-services <000000...111111> dscp <000000..111111> **(p. 385)**
    - **codepoint < 000000 | 000001 | 000010 | ... >** -- Configure the Type-of-Service method the device uses to prioritize IP traffic **(p. 384)**

  - **dscp < 000000 | 000001 | 000010 | ... >** -- Define Differentiated Services Codepoint to which to map IP ToS. **(p. 386)**
- **ip-precedence** -- In IP-Precedence mode, IPv4 packets are classified and given a QoS priority based on the upper 3 bits of the IP ToS field. The priority association is automatic and cannot be changed: IP-Precedence 802.1p ToS Bits Priority ------------------------------ 111 7 (Highest) 110 6 101 5 100 4 011 3 010 0 (Normal) 001 2 (Low) 000 1 (Lowest) **(p. 387)**

EXAMPLES

COMMAND DETAILS

2-queues

- qos queue-config 2-queues

```
Set the number of outbound port queues for all switch ports.
```

4-queues

- qos queue-config 4-queues

```
Set the number of outbound port queues for all switch ports.
```

8-queues

- qos queue-config 8-queues

```
Set the number of outbound port queues for all switch ports.
```

apptype

- [no] qos *< udp-port | tcp-port >*

```
Usage: [no] qos <udp|tcp> <TCP/UDP-PORT|range TCP/UDP-PORT MAX-TCP/UDP-PORT>
                          [dscp <000000|000001...111111> | priority <0-7>]

Description: Configure priorities for TCP/UDP services. The priority can
             be defined for packets sourced and destined to a particular
             TCP/UDP service. The specified priority value will be placed
             in the 802.1p priority field of outgoing tagged packets. The
             packets will also be placed in the appropriate outbound priority
             queue. '7' means highest priority.  If 'dscp' is specified, the
             priority of the outgoing packets is defined by the
             Differentiated Services Codepoint mapping (see 'show qos
             dscp-map'). Using 'no' removes any priority assignment for
             this TCP/UDP service.
             If MAX-TCP/UDP-PORT is specified then the priority is applied
             to all TCP/UDP ports in the range from TCP/UDP-PORT to
             MAX-TCP/UDP-PORT.
```

Supported Values:

- **udp-port** -- Set UDP port based priority.
- **tcp-port** -- Set TCP port based priority.

Next Available Options:

- **port-num** -- TCP/UDP port from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 388)**
- **range** -- Specify range of TCP/UDP ports from [to] which to prioritize traffic.**(p. 391)**

codepoint

- [no] qos type-of-service diff-services *< 000000 | 000001 | 000010 | ... >*

```
Usage: [no] type-of-service <ip-precedence|
                             diff-services <000000|000001...111111>
                             [dscp <000000|000001...111111>]>

Description: Configure the Type-of-Service method the device uses to
             prioritize IP traffic.  Prioritization is done based on the
             contents of the Type of Service (ToS) field in the IP header
             of each packet.  Using 'no' type-of-service with just the
             mode (ip-precedence or diff-services) will disable all ToS
             QoS for the switch.

Modes:
--------------
Disabled        The switch does NOT prioritize IP packets based on the IP
                ToS field.

IP Precedence   The switch uses the upper 3 bits of the IP ToS field (the IP
                Precedence bits) to determine the 802.1p priority of the
                packet and its outbound switch queue. If the packet is
                transmitted out a port on which VLAN tagging is enabled, the
                new priority is placed in the outbound VLAN tag. See the
                switch documentation for more information.

Differentiated  The switch uses the upper 6 bits of the ToS field (the
Services        Differentiated Services bits) to decide whether to apply an
                802.1p priority to the packet and thus affect its outbound
                queue. The priority is defined by the Differentiated
                Services Codepoint mapping (see 'show qos dscp-map'). If no
                priority is mapped for the packet's codepoint, the switch
                does not classify the packet using Differentiated Services.
                If there IS an associated priority configured, and the
                packet is transmitted out a port on which VLAN tagging is
                enabled, the new 802.1p priority will be placed in the
                outbound VLAN tag.  If a DSCP Policy is configured to apply
                to the inbound DS codepoint (i.e., the codepoint has been
                're-mapped'), the priority assignment and outbound queueing
                will be that specified by the new Policy's codepoint in the
                DSCP table, and the Differentiated Services field in the
                outbound packet will be changed to the new value.
                Using 'no type-of-service diff-services <000000...111111>'
                removes the re-mapping assignment, i.e., a new DSCP Policy
                will no longer be applied to the specified codepoint. To
                remove a priority association from a codepoint altogether,
                the  'no dscp-map <000000.111111>' function must be used.

    o diff-services <000000|000001...111111> - The value of the upper
      6 bits in the ToS field.

    o dscp <000000|000001...111111> - Re-maps a given inbound Differentiated
      Services codepoint to the specified DSCP Policy and codepoint on
      outbound.
```

Supported Values:

Binary formatted value from 000000 to 111111

Next Available Option:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Define Differentiated Services Codepoint to which to map IP ToS.**(p. 386)**

device-priority

- [no] qos device-priority *IP-ADDR*

```
Usage: [no] qos device-priority IP-ADDR [dscp <000000|000001...111111>|
                                         priority <0-7>]

Description: Configure device-based priority. The priority can be set for
             IP packets from/to a particular IP Address.  The specified
             priority value will be placed in the 802.1p priority field of
             outgoing tagged packets. The packets will also be placed in
             the appropriate outbound priority queue. '7' means highest
             priority. If 'dscp' is specified, the priority of the outgoing
             packets is defined by the Differentiated Services Codepoint
             mapping (see 'show qos dscp-map').  Using 'no' removes any
             priority assignment for this IP address.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 386)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 388)**

diff-services

- qos type-of-service diff-services

```
In IP Differentiated Services (Diffserv) mode, IPv4 packets are classified
      and given a QoS priority based on the upper 6 bits of the IP ToS
      field from the packets as they enter the switch.

      The assignment of Diffserv Codepoints to 802.1p priorities is done
      via the   qos dscp-map   command.

      Any Diffserv Codepoint in an inbound IPv4 packet can be re-mapped to
      a different codepoint (and its associated 802.1p priority) on
      outbound. This is done by using the syntax:

      qos type-of-service diff-services <000000...111111> dscp <000000..111111>
```

Next Available Option:

- **codepoint** < 000000 | 000001 | 000010 | ... > -- Configure the Type-of-Service method the device uses to prioritize IP traffic**(p. 384)**

dscp

- qos device-priority *IP-ADDR* dscp *< 000000 | 000001 | 000010 | ... >*

  ```
  Specify DSCP policy to use.
  ```

  Supported Values:

  Binary formatted value from 000000 to 111111
- qos *< udp-port | tcp-port > TCP/UDP-PORT* dscp *< 000000 | 000001 | 000010 | ... >*

  ```
  Specify DSCP policy to use.
  ```

  Supported Values:

  Binary formatted value from 000000 to 111111
- qos *< udp-port | tcp-port >* range *TCP/UDP-PORT TCP/UDP-PORT* dscp *< 000000 | 000001 | 000010 | ... >*

  ```
  Specify DSCP policy to use.
  ```

  Supported Values:

  Binary formatted value from 000000 to 111111
- qos type-of-service diff-services *< 000000 | 000001 | 000010 | ... >* dscp *< 000000 | 000001 | 000010 | ... >*

  ```
  Define Differentiated Services Codepoint to which to map IP ToS.
  ```

  Supported Values:

  Binary formatted value from 000000 to 111111

dscp-map

- [no] qos dscp-map *< 000000 | 000001 | 000010 | ... >*

```
Usage: [no] qos dscp-map <000000|000001...111111>
                         [priority <<0-7>|no-override>]
                         [name <str>]

Description: Define mapping between a DSCP (Differentiated-Services
             Codepoint) value and an 802.1p priority. The mapping is used
             to assign priority for IPv4 packets if a QoS classifier uses
             this DSCP policy as the method of traffic prioritization.

            The mapping also provides the profile for inbound classification
            and priority assignment based on an IPv4 packet's received
            IP ToS byte ONLY IF the user has also configured
                 'qos type-of-service diff-services'

             'no qos dscp-map <codepoint>' will remove the settings for the
             specified codepoint from the running configuration.  The
             priority is set to no-override and the name is deleted (the
             priority and name can only be removed if no QoS feature is
```

```
configured to use this DSCP Policy).

'no qos dscp-map <codepoint> name'  will remove the name
associated with this policy, but not the policy priority.

Certain codepoints may have a default associated 802.1p
priority, as part of the IETF standards for Assured Forwarding
and Expedited Forwarding. These are automatically configured as
follows:

   DiffServ       802.1p
   Codepoint       Value       IETF Standard Designation
   ---------------------------------------------------
   001010           1         Assured Forwarding   AF11
   001100           1         Assured Forwarding   AF12
   001110           2         Assured Forwarding   AF13
   010010           0         Assured Forwarding   AF21
   010100           0         Assured Forwarding   AF22
   010110           3         Assured Forwarding   AF23
   011010           4         Assured Forwarding   AF31
   011100           4         Assured Forwarding   AF32
   011110           5         Assured Forwarding   AF33
   100010           6         Assured Forwarding   AF41
   100100           6         Assured Forwarding   AF42
   100110           7         Assured Forwarding   AF43
   101110           7         Expedited Forwarding EF
```

Supported Values:

Binary formatted value from 000000 to 111111

Next Available Options:

- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 388)**
- **name** -- Specify DSCP->priority mapping name. **(p. 388)**

ip-precedence

- qos type-of-service ip-precedence

```
In IP-Precedence mode, IPv4 packets are classified and given a QoS priority
      based on the upper 3 bits of the IP ToS field. The priority
      association is automatic and cannot be changed:
             IP-Precedence      802.1p
               ToS Bits        Priority
             --------------------------------
                111              7 (Highest)
                110              6
                101              5
                100              4
                011              3
                010              0 (Normal)
                001              2 (Low)
                000              1 (Lowest)
```

max-port-num

- [no] qos *< udp-port | tcp-port >* range *TCP/UDP-PORT TCP/UDP-PORT*

  ```
  Maximal TCP/UDP port in the range from [to] which to prioritize traffic.
  ```

  Next Available Options:
  - **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 386)**
  - **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 388)**

name

- [no] qos dscp-map *< 000000 | 000001 | 000010 | ... >* name

  ```
  Specify DSCP->priority mapping name.
  ```

  Next Available Option:
  - **name-string** -- Specify DSCP->priority mapping name. (ASCII-STR) **(p. 388)**

name-string

- qos dscp-map *< 000000 | 000001 | 000010 | ... >* name *NAME-STRING*

  ```
  Specify DSCP->priority mapping name.
  ```

port-num

- qos *< udp-port | tcp-port >* *TCP/UDP-PORT*

  ```
  TCP/UDP port from [to] which to prioritize traffic.
  ```

  Next Available Options:
  - **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 386)**
  - **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 388)**

- qos *< udp-port | tcp-port >* range *TCP/UDP-PORT*

  ```
  TCP/UDP port from [to] which to prioritize traffic.
  ```

  Next Available Option:
  - **max-port-num** -- Maximal TCP/UDP port in the range from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 388)**

priority

- qos device-priority *IP-ADDR* priority *< 0 | 1 | 2 | ... >*

  ```
  Specify priority to use.
  ```

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**

    - **4**
    - **5**
    - **6**
    - **7**

- qos dscp-map *< 000000 | 000001 | 000010 | ... >* priority *< 0 | 1 | 2 | ... >*

  ```
  Specify priority to use.
  ```

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- qos protocol *< IP | IPX | ARP | ... >* priority *< 0 | 1 | 2 | ... >*

  ```
  Specify priority to use.
  ```

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- qos *< udp-port | tcp-port >* *TCP/UDP-PORT* priority *< 0 | 1 | 2 | ... >*

  ```
  Specify priority to use.
  ```

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- qos *< udp-port | tcp-port >* range *TCP/UDP-PORT TCP/UDP-PORT* priority *< 0 | 1 | 2 | ... >*

  ```
  Specify priority to use.
  ```

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**

- **7**

protocol

- [no] qos protocol *< IP | IPX | ARP | ... >*

```
Usage: [no] qos protocol <ip|ipx|arp|appletalk|sna|netbeui>
                         [priority <0-7>]

Description: Configure protocol-based priority. The priority can be
             defined for any of the listed protocol types. The specified
             priority value will be placed in the 802.1p priority field of
             outgoing tagged packets. The protocol packets will also be
             placed in the appropriate outbound priority queue. '7' means
             highest priority. Using 'no' removes any priority assignment
             for the specified protocol.
```

Supported Values:

- **IP**
- **IPX**
- **ARP**
- **AppleTalk**
- **SNA**
- **NetBEUI**

Next Available Option:

- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 388)**

queue-config

- qos queue-config

```
Usage: queue-config <2-queues|4-queues|8-queues>

Description: Sets the number of outbound port queues that buffer the
             packets depending on their 802.1p priority.  This command will
             execute a 'write memory', replacing the Startup configuration
             with the contents of the current Running configuration. The new
             configuration will reset the number of outbound port queues and
             remove any previously configured 'bandwidth-min output' settings.
             After the write memory is executed, the switch will reboot
             immediately.
             The mapping of 802.1p priorities to outbound port queues is
             shown below:

              802.1p
             Priority     | 2-queues | 4-queues | 8-queues
             --------------------------------------------
             1 (lowest)   |    1     |    1          1
             2            |    1     |    1          2
             0 (normal)   |    1     |    2          3
             3            |    1     |    2          4
             4            |    2     |    3          5
             5            |    2     |    3          6
             6            |    2     |    4          7
             7 (highest)  |    2     |    4          8
```

Next Available Options:

- **2-queues** -- Set the number of outbound port queues for all switch ports. **(p. 383)**
- **4-queues** -- Set the number of outbound port queues for all switch ports. **(p. 383)**
- **8-queues** -- Set the number of outbound port queues for all switch ports. **(p. 383)**

range

- qos *< udp-port | tcp-port >* range

```
Specify range of TCP/UDP ports from [to] which to prioritize traffic. A port
range can be from 1 to 65535 (inclusive) ports or any subset thereof. The
minimum port number must precede the maximum port number in the range.
Note: If you have specified a range of port numbers, you must specify the
entire range in the 'no' command; you cannot remove part of a range.
```

Next Available Option:

- **port-num** -- TCP/UDP port from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 388)**

Example 1. Example of Port Range

ProCurve(config)# qos udp-port range 1001 2000 dscp 000010

type-of-service

- [no] qos type-of-service

```
Usage: [no] type-of-service <ip-precedence|
                             diff-services <000000|000001...111111>
                             [dscp <000000|000001...111111>]>

Description: Configure the Type-of-Service method the device uses to
             prioritize IP traffic.  Prioritization is done based on the
             contents of the Type of Service (ToS) field in the IP header
             of each packet.  Using 'no' type-of-service with just the
             mode (ip-precedence or diff-services) will disable all ToS
             QoS for the switch.

Modes:
--------------
Disabled        The switch does NOT prioritize IP packets based on the IP
                ToS field.

IP Precedence   The switch uses the upper 3 bits of the IP ToS field (the IP
                Precedence bits) to determine the 802.1p priority of the
                packet and its outbound switch queue. If the packet is
                transmitted out a port on which VLAN tagging is enabled, the
                new priority is placed in the outbound VLAN tag. See the
                switch documentation for more information.

Differentiated  The switch uses the upper 6 bits of the ToS field (the
Services        Differentiated Services bits) to decide whether to apply an
                802.1p priority to the packet and thus affect its outbound
                queue. The priority is defined by the Differentiated
                Services Codepoint mapping (see 'show qos dscp-map'). If no
                priority is mapped for the packet's codepoint, the switch
                does not classify the packet using Differentiated Services.
                If there IS an associated priority configured, and the
                packet is transmitted out a port on which VLAN tagging is
                enabled, the new 802.1p priority will be placed in the
                outbound VLAN tag.  If a DSCP Policy is configured to apply
                to the inbound DS codepoint (i.e., the codepoint has been
                're-mapped'), the priority assignment and outbound queueing
                will be that specified by the new Policy's codepoint in the
                DSCP table, and the Differentiated Services field in the
                outbound packet will be changed to the new value.
                Using 'no type-of-service diff-services <000000...111111>'
                removes the re-mapping assignment, i.e., a new DSCP Policy
                will no longer be applied to the specified codepoint. To
                remove a priority association from a codepoint altogether,
                the  'no dscp-map <000000.111111>' function must be used.

      o diff-services <000000|000001...111111> - The value of the upper
        6 bits in the ToS field.

      o dscp <000000|000001...111111> - Re-maps a given inbound Differentiated
        Services codepoint to the specified DSCP Policy and codepoint on
        outbound.
```

Next Available Options:

- **ip-precedence** -- In IP-Precedence mode, IPv4 packets are classified and given a QoS priority based on the upper 3 bits of the IP ToS field. The priority association is automatic and cannot be changed: IP-Precedence 802.1p ToS Bits Priority -------------------------------- 111 7 (Highest) 110 6 101 5 100 4 011 3 010 0 (Normal) 001 2 (Low) 000 1 (Lowest) **(p. 387)**
- **diff-services** -- In IP Differentiated Services (Diffserv) mode, IPv4 packets are classified and given a QoS priority based on the upper 6 bits of the IP ToS field from the packets as they enter the switch. The assignment of Diffserv Codepoints to 802.1p priorities is done via the qos dscp-map command. Any Diffserv Codepoint in an inbound IPv4 packet can be re-mapped to a different codepoint (and its associated 802.1p priority) on outbound. This is done by using the syntax: qos type-of-service diff-services <000000...111111> dscp <000000..111111> **(p. 385)**

radius-server

OVERVIEW

Category:	Switch Security
Primary context:	config
Related Commands	**show radius (page 500)**

```
Usage:   [no] radius-server host <IP-ADDR>
                                 [auth-port <UDP-PORT>]
                                 [acct-port <UDP-PORT>]
                                 [dyn-authorization]
                                 [time-window <0-65535>]
                                 [key <KEY-STR>]
         [no] radius-server key <KEY-STR>
              radius-server timeout <1-15>
              radius-server retransmit <1-5>
              radius-server dyn-autz-port <UDP-PORT>
         [no] radius-server dead-time <1-1440>

Description: Configure RADIUS parameters.
             The first command adds/removes a RADIUS server to/from the
             list of the RADIUS servers that will be used for the
             authentication, accounting and authorization. Up to 3 RADIUS
             servers can be configured.
             The second command sets/removes the global encryption key to use
             in communication with RADIUS servers.
             The third command sets the interval in seconds the switch
             waits for a reply from a RADIUS server.
             The fourth command specifies the number of times the switch
             retransmits requests to a RADIUS server.
             The fifth command specifies the UDP port to listen for
             Change-of-Authorization and Disconnect messages.
             The last command sets the length of time in minutes a RADIUS
             server that failed to respond to an authentication request is
             bypassed by additional requests. See 'dead-time', below. Use
             the 'no' form of command to set the dead-time to 0.

Parameters:

    o host IP-ADDR [auth-port <UDP-PORT>] [acct-port <UDP-PORT>]
                   [dyn-authorization] [time-window <0-65535>]
                   [key <KEY-STR>] - specifies
              the IP address of the RADIUS server to use. Optional parameter
              'auth-port <UDP-PORT>' specifies the UDP destination port to use
              when sending authentication requests to the server (default is
              1812). Optional parameter 'acct-port <UDP-PORT>' specifies the
              UDP destination port to use when sending accounting requests to
              the server (default is 1813). Optional 'dyn-authorization'
              parameter enables/disables the processing of Disconnect and
              Change-of-Authorization messages from the host. Optional
              parameter 'time-window <0-65535>' specifies the time frame
              (in seconds) within which received Change-of-Authorization and
              Disconnect request messages will be considered current and
              accepted for processing, '0' value means 'infinity' (default is
              300 seconds). Optional parameter 'key <KEY-STR>' specifies an
```

```
                    encryption key to use for authentication with given server
                    (default is NULL). Specifying this key overrides the key set for
                    this server by the 'radius-server key <KEY-STR>' global
                    configuration command.
          o key <KEY-STR> - specifies the global encryption key, which is
                    used for authentication if encryption key for the server is
                    not configured. The default is NULL.
          o timeout <1-15> - server response timeout interval in seconds. The
                    default is 5 seconds.
          o retransmit <1-5> - specifies the maximum number of retransmission
                    attempts. The default is 3 attempts.
          o dyn-autz-port <UDP-PORT> - specifies the UDP port to listen for
                    Change-of-Authorization and Disconnect messages. The default
                    is 3799.
          o dead-time <1-1440> - If the switch does not receive a response from a
                    specific RADIUS server, the switch avoids sending any new
                    authentication requests to that server until the dead-time has
                    expired. That is, during a new authentication attempt, the
                    switch bypasses a specified RADIUS server if a dead-time
                    period is running on the switch for a previous failure to
                    receive a response from that server. (The switch will still
                    send new authentication requests to any other configured
                    RADIUS servers that are not affected by a dead-time
                    condition.) For a specific RADIUS server, dead-time counting
                    begins with the end of the last timeout in the last retransmit
                    attempt of the failed authentication session. When dead-time
                    is set to 0 (zero), there is no dead-time and the switch will
                    not bypass a RADIUS server that has failed to respond to an
                    earlier authentication attempt. (Default: 0.)
```

COMMAND STRUCTURE

- [no] radius-server **dead-time** **< Min | Max >** -- Server unavailability time (default is 0, use the 'no' form of command to set the dead-time to 0). **(p. 396)**
  - **dead-time** **< 1 to 1440 >** -- Server unavailability time (default is 0, use the 'no' form of command to set the dead-time to 0). **(p. 396)**
- radius-server **dyn-autz-port** **< 1024 to 49151 >** -- UDP port number to listen for Change-of-Authorization and Disconnect messages (default is 3799). (TCP/UDP-PORT) **(p. 396)**
- [no] radius-server **host** -- IP address of the RADIUS server to use. (IP-ADDR) **(p. 397)**
  - **acct-port** -- Accounting UDP destination port number (default is 1813). **(p. 395)**
    - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 395)**
      - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 395)**
      - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**
  - **auth-port** -- Authentication UDP destination port number (default is 1812). **(p. 395)**
    - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 395)**
      - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 395)**
      - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**
  - **dyn-authorization** -- Enable/disable dynamic authorization control from this host. **(p. 396)**
  - **key** -- Encryption key to use with the RADIUS server (default is NULL). **(p. 397)**
    - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**

        - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 395)**
        - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 395)**
    - **time-window** -- time window (in seconds) within which the received dynamic authorization requests are considered to be current and accepted for processing. **(p. 398)**
        - **time-window < 0 to 65535 >** -- **(p. 398)**
- [no] radius-server **key** -- Global encryption key (default is NULL). **(p. 397)**
    - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**
- radius-server **retransmit < 1 to 5 >** -- Number of packet retransmits (default is 3). **(p. 397)**
- radius-server **timeout < 1 to 15 >** -- Server timeout interval (default is 5). **(p. 398)**

EXAMPLES

COMMAND DETAILS

acct-port (p. 395)
auth-port (p. 395)
dead-time (p. 396)
dyn-authorization (p. 396)
dyn-autz-port (p. 396)
host (p. 397)
key (p. 397)
retransmit (p. 397)
timeout (p. 398)
time-window (p. 398)

acct-port

- radius-server host *IP-ADDR* acct-port

```
Accounting UDP destination port number (default is 1813).
```

Next Available Option:

- **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 395)**

- radius-server host *IP-ADDR* acct-port *TCP/UDP-PORT*

```
Accounting UDP destination port number (default is 1813).
```

Next Available Options:

- **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 395)**
- **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**

- radius-server host *IP-ADDR* auth-port *TCP/UDP-PORT* acct-port *TCP/UDP-PORT*

```
Accounting UDP destination port number (default is 1813).
```

- radius-server host *IP-ADDR* key *KEY* acct-port *TCP/UDP-PORT*

```
Accounting UDP destination port number (default is 1813).
```

auth-port

- radius-server host *IP-ADDR* acct-port *TCP/UDP-PORT* auth-port *TCP/UDP-PORT*

```
Authentication UDP destination port number (default is 1812).
```

- radius-server host *IP-ADDR* auth-port

```
Authentication UDP destination port number (default is 1812).
```

Next Available Option:

- **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 395)**

- radius-server host *IP-ADDR* auth-port *TCP/UDP-PORT*

```
Authentication UDP destination port number (default is 1812).
```

Next Available Options:

- **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 395)**
- **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**

- radius-server host *IP-ADDR* key *KEY* auth-port *TCP/UDP-PORT*

```
Authentication UDP destination port number (default is 1812).
```

dead-time

- [no] radius-server dead-time

```
Server unavailability  time (default is 0, use the 'no'
form of command to set the dead-time to 0).
```

Supported Values:

- **Min**
- **Max**

Next Available Option:

- **dead-time** < 1 to 1440 > -- Server unavailability time (default is 0, use the 'no' form of command to set the dead-time to 0).**(p. 396)**

- radius-server dead-time *< 1 to 1440 >*

```
Server unavailability  time (default is 0, use the 'no'
form of command to set the dead-time to 0).
```

Range: < 1 to 1440 >

dyn-authorization

- [no] radius-server host *IP-ADDR* dyn-authorization

```
Enable/disable dynamic authorization control from this host.
```

dyn-autz-port

- radius-server dyn-autz-port *< 1024 to 49151 >*

```
UDP port number to listen for Change-of-Authorization and Disconnect messages
 (default is 3799).
```

Range: < 1024 to 49151 >

host

- [no] radius-server host *IP-ADDR*

  ```
  IP address of the RADIUS server to use.
  ```

  Next Available Options:
  - **acct-port** -- Accounting UDP destination port number (default is 1813).**(p. 395)**
  - **auth-port** -- Authentication UDP destination port number (default is 1812).**(p. 395)**
  - **dyn-authorization** -- Enable/disable dynamic authorization control from this host.**(p. 396)**
  - **time-window** -- time window (in seconds) within which the received dynamic authorization requests are considered to be current and accepted for processing. **(p. 398)**
  - **key** -- Encryption key to use with the RADIUS server (default is NULL).**(p. 397)**

key

- radius-server host *IP-ADDR* acct-port *TCP/UDP-PORT* key *KEY*

  ```
  Encryption key to use with the RADIUS server (default is NULL).
  ```

- radius-server host *IP-ADDR* auth-port *TCP/UDP-PORT* key *KEY*

  ```
  Encryption key to use with the RADIUS server (default is NULL).
  ```

- [no] radius-server host *IP-ADDR* key

  ```
  Encryption key to use with the RADIUS server (default is NULL).
  ```

  Next Available Option:
  - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**

- radius-server host *IP-ADDR* key *KEY*

  ```
  Encryption key to use with the RADIUS server (default is NULL).
  ```

  Next Available Options:
  - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 395)**
  - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 395)**

- [no] radius-server key

  ```
  Global encryption key (default is NULL).
  ```

  Next Available Option:
  - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 397)**

- radius-server key *KEY*

  ```
  Encryption key to use with the RADIUS server (default is NULL).
  ```

retransmit

- radius-server retransmit *< 1 to 5 >*

```
Number of packet retransmits (default is 3).
```

Range: < 1 to 5 >

timeout

- radius-server timeout *< 1 to 15 >*

  ```
  Server timeout interval (default is 5).
  ```

  Range: < 1 to 15 >

time-window

- [no] radius-server host *IP-ADDR* time-window

  ```
  time window (in seconds) within which the received dynamic authorization
  requests are considered to be current and accepted for processing.
  ```

  Next Available Option:

  - **time-window** < 0 to 65535 > -- **(p. 398)**

- radius-server host *IP-ADDR* time-window *< 0 to 65535 >*

  Range: < 0 to 65535 >

redo

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**repeat (page 406)**

```
Usage: redo [NUMBER|COMMAND-STR]

Description: Re-execute a command from history.
             By default, it executes the last command. If the 'number' is
             specified, it executes the n-th command starting from the most
             recent command in the history. The n is the number specified.
             If the 'COMMAND-STR' is specified, it executes the most recent
             command whose name matches the specified string.
```

COMMAND STRUCTURE

- redo **command** -- The command word identifying a command to execute in the history list. (ASCII-STR) **(p. 399)**
- redo **NUMBER** -- The position of the command to execute in the history list. (NUMBER) **(p. 399)**

COMMAND DETAILS

command (p. 399)	**NUMBER (p. 399)**

command

- redo *COMMAND*

```
The command word identifying a command to execute in the history list.
```

NUMBER

- redo *NUMBER*

```
The position of the command to execute in the history list.
```

redundancy

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: redundancy switchover
       redundancy active-management < management-module1 |
                                      management-module2 |
                                      standby>
       [no]redundancy management-module
       redundancy  fabric-module <<1|2> <enable|disable>>

Description: Redundancy configuration for management and fabric modules.
             The first version of the command causes the switch to
             immediately switchover to the standby management module.
             The second version of the command makes the module specified
             an active management module for next boot. This command
             will fail if the other module is in a failed state.
             The third version of the command enables/disables
             redundant management. The current 'active' management module
             will continue to be the 'active' management module on boot,
             unless the user uses the 'redundancy active-management ...'
             command to change to the other module.
             The fourth version of the command enables/disables the fabric
             modules.
```

NOTES

Multiple Contexts

This command also is available in the manager context.

COMMAND STRUCTURE

- redundancy **active-management** **< management-module1 | management-module2 | standby >** -- Specify the management module that will be active for next boot. (NUMBER) **(p. 400)**
- redundancy **fabric-module** **< 1 | 2 >** -- Enable/Disable fabric modules. (NUMBER) **(p. 401)**
  - **disable** -- Disable the fabric module. **(p. 401)**
  - **enable** -- Enable the fabric module. **(p. 401)**
- [no] redundancy **management-module** -- Enable/Disable redundant management. **(p. 401)**
- redundancy **switchover** -- Switchover to the standby management module. **(p. 401)**

COMMAND DETAILS

active-management (p. 400)	**enable (p. 401)**	**management-module (p. 401)**
disable (p. 401)	**fabric-module (p. 401)**	**switchover (p. 401)**

active-management

- redundancy active-management *< management-module1 | management-module2 | standby >*

```
Specify the management module that will be active for next boot.
```

Supported Values:

- **management-module1** -- Configures management-module 1 as an active management module for next boot
- **management-module2** -- Configures management-module 2 as an active management module for next boot
- **standby** -- Configures standby module as an active management module for next boot

disable

- redundancy fabric-module *< 1 | 2 >* disable

```
Disable the fabric module.
```

enable

- redundancy fabric-module *< 1 | 2 >* enable

```
Enable the fabric module.
```

fabric-module

- redundancy fabric-module *< 1 | 2 >*

```
Enable/Disable fabric modules.
```

Supported Values:

- **1** -- enable/disable fabric module-1
- **2** -- enable/disable fabric module-2

Next Available Options:

- **enable** -- Enable the fabric module.**(p. 401)**
- **disable** -- Disable the fabric module.**(p. 401)**

management-module

- [no] redundancy management-module

```
Enable/Disable redundant management.
```

switchover

- redundancy switchover

```
Switchover to the standby management module.
```

redundancy

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: redundancy switchover
       redundancy active-management < management-module1 |
                                      management-module2 |
                                      standby>

Description: Redundancy configuration for management modules.
             The first version of the command causes the switch to
             immediately switchover to the standby management module.
             The second version of the command makes the module specified
             an active management module for next boot. This command
             will fail if the other module is in a failed state.
```

NOTES

Multiple Contexts

This command also is available in the config context.

COMMAND STRUCTURE

- redundancy active-management **< management-module1 | management-module2 | standby >** -- Specify the management module that will be active for next boot. (NUMBER) (p. 402)
- redundancy switchover -- Switchover to the standby management module. (p. 402)

COMMAND DETAILS

active-management (p. 402)	switchover (p. 402)

active-management

- redundancy active-management *< management-module1 | management-module2 | standby >*

```
Specify the management module that will be active for next boot.
```

Supported Values:

- **management-module1** -- Configures management-module 1 as an active management module for next boot
- **management-module2** -- Configures management-module 2 as an active management module for next boot
- **standby** -- Configures standby module as an active management module for next boot

switchover

- redundancy switchover

```
Switchover to the standby management module.
```

reload

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**boot (page 67)**

```
Usage: [no] reload <after  <[[DD:]HH:]MM>  |
                    at  HH:MM[:SS]  [MM/DD[/[YY]YY]>] >

Description: Warm reboot of the switch. If no parameters are entered,
             an immediate reload is executed.
             [no] - Causes the removal of any pending reload request.

             Note:  The maximum allowable time is 99 days.

Parameters:
        o after  - Warm reboot the switch after the given amount of
                   time has passed.
        o at     - Warm reboot the switch at the given time.
```

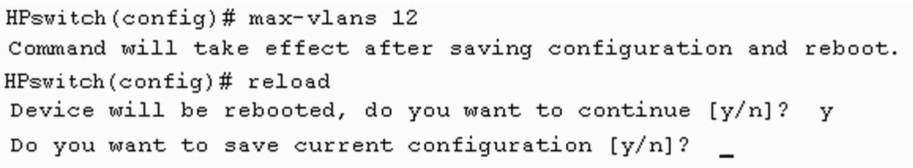
COMMAND STRUCTURE

- reload **after** -- Warm reboot in a specified amount of time. ([[DD:]HH:]MM) **(p. 403)**
- reload **at** -- Warm reboot at a specified time; If the mm/dd/yy is left blank, the current day is assumed. **(p. 404)**
  - **time** -- Time on given date to do a warm reboot. (HH:MM[:SS]) **(p. 404)**
    - **date** -- Date on which a warm reboot is to occur. (MM/DD[/[YY]YY]) **(p. 404)**

EXAMPLES

Example: reload

Automatically save your configuration changes and reboot the switch from the same flash image you have been using:



```
HPswitch(config)# max-vlans 12
Command will take effect after saving configuration and reboot.
HPswitch(config)# reload
Device will be rebooted, do you want to continue [y/n]?  y
Do you want to save current configuration [y/n]? _
```

COMMAND DETAILS

after (p. 403)	**date (p. 404)**
at (p. 404)	**time (p. 404)**

after

- reload after *[[DD:]HH:]MM*

```
Warm reboot in a specified amount of time.
```

at

- reload at

```
Warm reboot at a specified time; If the mm/dd/yy is left blank, the current day is
assumed.
```

Next Available Option:

- **time** -- Time on given date to do a warm reboot. (HH:MM[:SS]) **(p. 404)**

date

- reload at *[TIME]* *[DATE]*

```
Date on which a warm reboot is to occur.
```

time

- reload at *[TIME]*

```
Time on given date to do a warm reboot.
```

Next Available Option:

- **date** -- Date on which a warm reboot is to occur. (MM/DD[/[YY]YY]) **(p. 404)**

rename

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show config (page 462)** **erase (page 166)**

```
Usage: rename config OLDNAME NEWNAME

Description: Change the name of the configuration OLDNAME to NEWNAME.
             No action occurs if there is no configuration named
             OLDNAME, or if a configuration named NEWNAME already
             exists.
```

COMMAND STRUCTURE

- rename **config** **< config | new >** -- Change the name of the configuration OLDNAME to NEWNAME **(p. 405)**
  - **newname** -- Specify new name for configuration file. (ASCII-STR) **(p. 405)**

COMMAND DETAILS

config (p. 405)	**newname (p. 405)**

config

- rename config *< config | new >*

```
Usage: rename config OLDNAME NEWNAME

Description: Change the name of the configuration OLDNAME to NEWNAME.
             No action occurs if there is no configuration named
             OLDNAME, or if a configuration named NEWNAME already
             exists.
```

Supported Values:
- **config**
- **new**

Next Available Option:
- **newname** -- Specify new name for configuration file. (ASCII-STR) **(p. 405)**

newname

- rename config *< config | new > NEWNAME*

```
Specify new name for configuration file.
```

repeat

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**redo (page 399)**

```
Usage: repeat [NUMBER] [count NUMBER] [delay NUMBER]

Description: Repeat execution of a previous command.
             By default, repeats the last command until a key is pressed.
             If the 'NUMBER' is specified, repeats the n-th most recent
             command where n is the number.
             If the 'count NUMBER' is specified repeat the command
             the NUMBER of times.
             If the 'delay NUMBER' is specified, the iterations are
             separated by the NUMBER of seconds.
```

COMMAND STRUCTURE

- repeat **count** -- Number of repetitions to make. (NUMBER) **(p. 406)**
- repeat **delay** -- Delay between the command executions. (NUMBER) **(p. 406)**
- repeat **NUMBER** -- Specify the position of the command to execute in the history list. (NUMBER) **(p. 406)**

COMMAND DETAILS

count (p. 406)	**delay (p. 406)**	**NUMBER (p. 406)**

count

- repeat count *NUMBER*

```
Number of repetitions to make.
```

delay

- repeat delay *NUMBER*

```
Delay between the command executions.
```

NUMBER

- repeat *NUMBER*

```
Specify the position of the command to execute in the history list.
```

router

OVERVIEW

Category:	Routing
Primary context:	config
Related Commands	**ip (page 269)** **vlan (page 611)** **show ip (page 480)**

```
Usage: [no] router ...

Description: Configure the switch routing protocols. You can enter the commands from the
 global
            configuration context or the RIP, OSPF, PIM, or VRRP configuration contexts.

            For example, to enter an OSPF command from the global configuration context,

             use the "router" keyword in front of the command. To enter an OSPF
             command in the OSPF configuration context, type "router ospf" to change
             to the OSPF configuration context, then type the command without the
             "router" keyword.

             Use 'router ?' to see a list of all possible options.
```

COMMAND STRUCTURE

- [no] router **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the device, or enter OSPF Configuration Context **(p. 419)**
  - **area** -- Define/remove an OSPF area, area range or virtual link **(p. 410)**
    - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 411)**
      - **normal** -- Define a "normal" area. **(p. 418)**
      - **nssa < 0 to 16777215 >** -- Define a "not-so-stubby" area (or NSSA) and its cost. **(p. 418)**
        - **metric-type < type1 | type2 >** -- Metric type of the type-7 default. **(p. 417)**
        - **no-summary** -- Do not send summary LSA into the area. **(p. 418)**
      - **range** -- Summarize routes matching address/mask pair. **(p. 420)**
        - **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 416)**
        - **no-advertise** -- Do not advertise the range outside the area. **(p. 417)**
        - **type < summary | nssa >** -- Link state database type to apply the range. **(p. 427)**
      - **stub** -- Define a "stub" area and specify its cost. **(p. 424)**
        - **cost < 0 to 16777215 >** -- Enter cost to use when injecting default routes into the area. **(p. 413)**
        - **no-summary** -- Do not send summary LSA into the area. **(p. 418)**
      - **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 427)**
        - **authentication** -- Disable authentication. **(p. 411)**
        - **authentication-key** -- Set simple authentication method and key. **(p. 411)**
          - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 411)**
        - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 414)**
        - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 415)**
        - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 417)**
          - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 413)**

        - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 421)**
        - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 424)**
    - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 412)**
      - **normal** -- Define a "normal" area. **(p. 418)**
      - **nssa < 0 to 16777215 >** -- Define a "not-so-stubby" area (or NSSA) and its cost. **(p. 418)**
        - **metric-type < type1 | type2 >** -- Metric type of the type-7 default. **(p. 417)**
        - **no-summary** -- Do not send summary LSA into the area. **(p. 418)**
      - **range** -- Summarize routes matching address/mask pair. **(p. 420)**
        - **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 416)**
        - **no-advertise** -- Do not advertise the range outside the area. **(p. 417)**
        - **type < summary | nssa >** -- Link state database type to apply the range. **(p. 427)**
      - **stub** -- Define a "stub" area and specify its cost. **(p. 424)**
        - **cost < 0 to 16777215 >** -- Enter cost to use when injecting default routes into the area. **(p. 413)**
        - **no-summary** -- Do not send summary LSA into the area. **(p. 418)**
      - **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 427)**
        - **authentication** -- Disable authentication. **(p. 411)**
        - **authentication-key** -- Set simple authentication method and key. **(p. 411)**
          - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 411)**
        - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 414)**
        - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 415)**
        - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 417)**
          - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 413)**
        - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 421)**
        - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 424)**
  - **default-metric < 0 to 16777215 >** -- The default metric used for advertising external routes imported into OSPF by this router **(p. 414)**
  - **distance** -- Set administrative distance to associate with intra-area, inter-area and AS-external routes learned by OSPF **(p. 414)**
    - **external < 1 to 255 >** -- Set administrative distance to associate with external routes learned by OSPF. **(p. 415)**
    - **inter-area < 1 to 255 >** -- Set administrative distance to associate with inter-area routes learned by OSPF. **(p. 416)**
    - **intra-area < 1 to 255 >** -- Set administrative distance to associate with intra-area routes learned by OSPF. **(p. 416)**
  - **metric-type < type1 | type2 >** -- The default metric type used for advertising external routes imported into OSPF by this router **(p. 417)**
  - **redistribute < connected | static | rip >** -- Specify source protocols which will be redistributed into OSPF **(p. 420)**
  - **restrict** -- Prevent redistribution of routes via OSPF **(p. 421)**
    - **ip-addr** -- Prevent redistribution of routes via OSPF (IP-ADDR/MASK-LENGTH) **(p. 416)**
  - **rfc1583-compatibility** -- Enable/disable RFC-1583 compatibility **(p. 421)**
  - **trap < virtual-interface-state-change | neighbor-state-change | virtual-neighbor-state-change | ... >** -- Enable/disable OSPF traps **(p. 425)**
- [no] router **pim** -- Enable/disable/configure PIM protocol on the device, or enter PIM Configuration Context **(p. 419)**
  - **bsr-candidate** -- Configure the router to advertise itself as the Candidate Bootstrap Router (Candidate-BSR) for a PIM-SM domain **(p. 412)**

        - **bsm-interval < 5 to 300 >** -- Specify the interval for sending Bootstrap messages on PIM-SM interfaces. **(p. 412)**
        - **hash-mask-length < 1 to 32 >** -- Specify the length (in bits) of the hash mask. **(p. 415)**
        - **priority < 0 to 255 >** -- Specify the priority for the Candidate Bootstrap router. **(p. 420)**
        - **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-BSR router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 424)**
    - **join-prune-interval < 5 to 65535 >** -- Configure interval at which the router will send periodic PIM-SM Join/Prune messages **(p. 417)**
    - **rp-address** -- Statically configure the Rendezvous Point (RP) to accept multicast traffic for specified group or range of groups **(p. 422)**
        - **IP-ADDR** -- Specify the IP address of the static RP. (IP-ADDR) **(p. 416)**
            - **GROUP-ADDR/GROUP-MASK** -- Specify the range of multicast group addresses associated with the static RP. (IP-ADDR/MASK-LENGTH) **(p. 415)**
                - **override** -- Specify whether or not static RP configuration precedes the information learned by a BSR. **(p. 419)**
    - **rp-candidate** -- Configure router to advertise itself as the Candidate Rendezvous Point (Candidate-RP) to the Bootstrap Router (BSR) **(p. 423)**
        - **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 415)**
            - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 415)**
        - **hold-time < 30 to 255 >** -- Specify the hold time value to be send in C-RP-Adv messages. **(p. 416)**
        - **priority < 0 to 255 >** -- Specify the priority for the Candidate-RP router. **(p. 420)**
        - **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-RP router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 424)**
            - **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 415)**
                - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 415)**
    - **spt-threshold** -- Specify whether switching to the Shortest Path Tree is enabled or disabled on the router **(p. 424)**
    - **state-refresh < 10 to 300 >** -- Set the interval between successive State Refresh messages originated by this router **(p. 424)**
    - **trap < neighbor-loss | hardware-mrt-full | software-mrt-full | ... >** -- Enable/disable PIM traps **(p. 425)**
- [no] router **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the device, or enter RIP Configuration Context **(p. 422)**
    - **auto-summary** -- Enable/disable advertisement of summarized routes **(p. 412)**
    - **default-metric < 1 to 15 >** -- Set default metric for imported routes **(p. 414)**
    - **distance < 1 to 255 >** -- Set administrative distance for routes learned via RIP **(p. 414)**
    - **redistribute < connected | static | ospf >** -- Specify source protocols which will be redistributed into RIP **(p. 420)**
    - **restrict** -- Prevent redistribution of routes via RIP **(p. 421)**
        - **ip-addr** -- Prevent redistribution of routes via RIP (IP-ADDR/MASK-LENGTH) **(p. 416)**
- [no] router **vrrp** -- Enable/disable/configure Virtual Router Redundancy Protocol (VRRP) on the device **(p. 428)**
    - **traps** -- Enable/disable generation of VRRP traps **(p. 426)**

COMMAND DETAILS

area (p. 410)
area-id (p. 411)
hold-time (p. 416)
inter-area (p. 416)
redistribute (p. 420)
restrict (p. 421)

area

- [no] router ospf area

```
Usage:    area <OSPF-AREA-ID|backbone> [normal]
          area <OSPF-AREA-ID|backbone> nssa <0-16777215>
                             [metric-type <type1|type2>] [no-summary]
          area <OSPF-AREA-ID|backbone> stub <0-16777215> [no-summary]
          area <OSPF-AREA-ID|backbone> range IP-ADDR/MASK-LENGTH
                                       [no-advertise]
          area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       [transit-delay <0-3600>]
                                       [retransmit-interval <0-3600>]
                                       [hello-interval <1-65535>]
                                       [dead-interval <0-2147483647>]
          area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       authentication-key OCTET-STR
          area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       md5-auth-key-chain CHAIN-NAME-STR
       no area <OSPF-AREA-ID|backbone>
       no area <OSPF-AREA-ID|backbone> range IP-ADDR/MASK-LENGTH
       no area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       [authentication]

Description: Define/remove an OSPF area, area range or virtual link.
           - 'area... [normal]' command defines a normal area. Area can be
             identified by a single integer or an IP address style dotted
             decimal. Use 0.0.0.0 address or 'backbone' keyword to specify the
             backbone area.
           - 'area... nssa...' defines a "not-so-stubby" area (or NSSA)
             and its cost. You can specify also the metric type and/or disable
             summary LSA to be sent into the area.
           - 'area... stub...' defines a "stub" area and cost to use when
             injecting default routes of a border router into the area. If
             'no-summary' is specified then no summary LSA will be sent into
             the area.
           - 'area... range...' defines a range of IP addresses the area
             consists of and directs to summarize routes matching the range.
             If 'no-advertise' is specified then the range will not be
             advertised outside the area.
```

```
- 'area... virtual-link...' defines a virtual link along with its
  time duration parameters:
  'transit-delay' - The estimated number of seconds it takes to
  transmit a link state update packet over the link.
  'retransmit-interval' - The number of seconds between link-state
  advertisement retransmissions. This value is also used when
  retransmitting database description and link-state request packets.
  'hello-interval' - The number of seconds between the Hello packets
  those the router sends to the virtual neighbor.
  'dead-interval' - The number of seconds that a router's Hello
  packets have not been seen before it's neighbor declares the
  router down. This should be some multiple of the Hello interval.
- 'area... virtual-link... authentication-key...' - specifies the
  authentication key to be used to maintain the virtual link. Note
  that unauthenticated link need no authentication key, and simple
  password authentication cannot use a key of more than 8 octets.
- 'area... virtual-link... md5-auth-key-chain...' -
  specifies the key chain to pick keys for MD5 authentication
  from and configures the virtual link to MD5 authentication.
- 'no area...' removes the entire area.
- 'no area... range...' removes the specified range.
- 'no area... virtual-link...' removes the specified virtual link,
  and 'no area... virtual-link... authentication' unsets the
  authentication on the link.
```

Next Available Options:

- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 411)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 412)**

area-id

- router ospf area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

Next Available Options:

- **normal** -- Define a "normal" area.**(p. 418)**
- **nssa** < 0 to 16777215 > -- Define a "not-so-stubby" area (or NSSA) and its cost.**(p. 418)**
- **stub** -- Define a "stub" area and specify its cost.**(p. 424)**
- **range** -- Summarize routes matching address/mask pair.**(p. 420)**
- **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 427)**

authentication

- [no] router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* authentication

```
Disable authentication.
```

- [no] router ospf area backbone virtual-link *IP-ADDR* authentication

```
Disable authentication.
```

authentication-key

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* authentication-key

```
Set simple authentication method and key.
```

Next Available Option:

- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 411)**

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

- router ospf area backbone virtual-link *IP-ADDR* authentication-key

```
Set simple authentication method and key.
```

Next Available Option:

- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 411)**

- router ospf area backbone virtual-link *IP-ADDR* authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

auto-summary

- [no] router rip auto-summary

```
Usage: [no] auto-summary

Description: Enable/disable advertisement of summarized routes.
             Summarization mechanisms should be disabled when using both
             version 1 and version 2 of RIP within a single network.
```

backbone

- router ospf area backbone

```
The backbone area (the same as 0.0.0.0).
```

Next Available Options:

- **normal** -- Define a "normal" area.**(p. 418)**
- **nssa** < 0 to 16777215 > -- Define a "not-so-stubby" area (or NSSA) and its cost.**(p. 418)**
- **stub** -- Define a "stub" area and specify its cost.**(p. 424)**
- **range** -- Summarize routes matching address/mask pair.**(p. 420)**
- **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 427)**

bsm-interval

- router pim bsr-candidate bsm-interval *< 5 to 300 >*

```
Specify the interval for sending Bootstrap messages on PIM-SM interfaces.
```

Range: < 5 to 300 >

bsr-candidate

- [no] router pim bsr-candidate

```
Usage: bsr-candidate [source-ip-vlan <VLAN-ID>]
                     [hash-mask-length <1-32>]
                     [priority <0-255>]
                     [bsm-interval <5-300>]
```

```
    no bsr-candidate [source-ip-vlan <VLAN-ID>]

Description: Configure the router to advertise itself as the Candidate
             Bootstrap Router (Candidate-BSR) for a PIM-SM domain. When
             enabling router to be a Candidate-BSR the VLAN ID must be
             specified, which IP address will be advertised as a
             Candidate-BSR address. PIM-SM must be enabled on the VLAN.
             Use 'no' form of this command to disable the router to be a
             Candidate-BSR.
             NOTE: It is recommended that the same routing switch is
                   configured as both the Candidate-BSR and the Candidate-RP.
Parameters:

    o source-ip-vlan <VLAN-ID> - The VLAN which IP address will be advertised
             as the Candidate-BSR IP address.
    o hash-mask-length <1-32> - The mask length (in bits) used by the
             PIM-SM hash function when selecting an RP. The default is 30.
    o priority <0-255> - The priority for the Candidate-BSR for the
             local PIM-SM domain. The larger value means the higher priority.
             The default is 0.
    o bsm-interval <5-300> - The interval (in seconds) for sending periodic
             Bootstrap messages on all PIM-SM interfaces, when this router is
             the elected BSR. The default is 60 seconds.
```

Next Available Options:

- **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-BSR router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 424)**
- **hash-mask-length** < 1 to 32 > -- Specify the length (in bits) of the hash mask. **(p. 415)**
- **priority** < 0 to 255 > -- Specify the priority for the Candidate Bootstrap router. **(p. 420)**
- **bsm-interval** < 5 to 300 > -- Specify the interval for sending Bootstrap messages on PIM-SM interfaces. **(p. 412)**

chain-name

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- router ospf area backbone virtual-link *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

cost

- router ospf area *OSPF-AREA-ID* stub *< 0 to 16777215 >*

```
Enter cost to use when injecting default routes
into the area.
```

Range: < 0 to 16777215 >

- router ospf area backbone stub *< 0 to 16777215 >*

```
Enter cost to use when injecting default routes
into the area.
```

Range: < 0 to 16777215 >

dead-interval

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >
- router ospf area backbone virtual-link *IP-ADDR* dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >

default-metric

- router ospf default-metric *< 0 to 16777215 >*

  ```
  Usage: default-metric <0-16777215>

  Description: The default metric used for advertising external routes imported
               into OSPF by this router.
  ```

  Range: < 0 to 16777215 >
- router rip default-metric *< 1 to 15 >*

  ```
  Usage: default-metric <1-15>

  Description: Set default metric for imported routes.
               Default value is 1.
  ```

  Range: < 1 to 15 >

distance

- router ospf distance

  ```
  Usage: distance <intra-area|inter-area|external> <1-255>

  Description: Set administrative distance to associate with intra-area,
               inter-area and AS-external routes learned by OSPF. Default
               value is 110 for all types of OSPF routes.
  ```

  Next Available Options:
  - **intra-area** < 1 to 255 > -- Set administrative distance to associate with intra-area routes learned by OSPF.**(p. 416)**
  - **inter-area** < 1 to 255 > -- Set administrative distance to associate with inter-area routes learned by OSPF.**(p. 416)**
  - **external** < 1 to 255 > -- Set administrative distance to associate with external routes learned by OSPF.**(p. 415)**

- router rip distance *< 1 to 255 >*

  ```
  Usage: distance <1-255>

  Description: Set administrative distance for routes learned via RIP.
               Default value is 120.
  ```

  Range: < 1 to 255 >

external

- [no] router ospf distance external *< 1 to 255 >*

  `Set administrative distance to associate with external routes learned by OSPF.`

  Range: < 1 to 255 >

GROUP-ADDR/GROUP-MASK

- [no] router pim rp-address *IP-ADDR IP-ADDR/MASK-LENGTH*

  `Specify the range of multicast group addresses associated with the static RP.`

  Next Available Option:
  - **override** -- Specify whether or not static RP configuration precedes the information learned by a BSR. **(p. 419)**

- router pim rp-candidate source-ip-vlan *VLAN-ID* group-prefix *IP-ADDR/MASK-LENGTH*

  `Enter the address and mask to define the multicast group range.`

- router pim rp-candidate group-prefix *IP-ADDR/MASK-LENGTH*

  `Enter the address and mask to define the multicast group range.`

group-prefix

- router pim rp-candidate source-ip-vlan *VLAN-ID* group-prefix

  `Specify the multicast group prefix to associate with the Candidate-RP router.`

  Next Available Option:
  - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 415)**

- [no] router pim rp-candidate group-prefix

  `Specify the multicast group prefix to associate with the Candidate-RP router.`

  Next Available Option:
  - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 415)**

hash-mask-length

- router pim bsr-candidate hash-mask-length *< 1 to 32 >*

  `Specify the length (in bits) of the hash mask.`

  Range: < 1 to 32 >

hello-interval

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* hello-interval *< 1 to 65535 >*

  `Set hello interval in seconds; the default is 10.`

  Range: < 1 to 65535 >

- router ospf area backbone virtual-link *IP-ADDR* hello-interval *< 1 to 65535 >*

  ```
  Set hello interval in seconds; the default is 10.
  ```

  Range: < 1 to 65535 >

hold-time

- router pim rp-candidate hold-time *< 30 to 255 >*

  ```
  Specify the hold time value to be send in C-RP-Adv messages.
  ```

  Range: < 30 to 255 >

inter-area

- [no] router ospf distance inter-area *< 1 to 255 >*

  ```
  Set administrative distance to associate with inter-area routes learned by OSPF.
  ```

  Range: < 1 to 255 >

intra-area

- [no] router ospf distance intra-area *< 1 to 255 >*

  ```
  Set administrative distance to associate with intra-area routes learned by OSPF.
  ```

  Range: < 1 to 255 >

ip

- router ospf area *OSPF-AREA-ID* range *IP-ADDR/MASK-LENGTH*

  ```
  Specify IP address/mask pair.
  ```

- router ospf area backbone range *IP-ADDR/MASK-LENGTH*

  ```
  Specify IP address/mask pair.
  ```

ip-addr

- [no] router ospf restrict *IP-ADDR/MASK-LENGTH*

  ```
  Usage: [no] restrict IP-ADDR/MASK-LEN

  Description: Prevent redistribution of routes via OSPF.
  ```

- [no] router rip restrict *IP-ADDR/MASK-LENGTH*

  ```
  Usage: [no] restrict IP-ADDR/MASK-LEN

  Description: Prevent redistribution of routes via RIP.
  ```

IP-ADDR

- [no] router pim rp-address *IP-ADDR*

  ```
  Specify the IP address of the static RP.
  ```

  Next Available Option:

  - **GROUP-ADDR/GROUP-MASK** -- Specify the range of multicast group addresses associated with the static RP. (IP-ADDR/MASK-LENGTH) **(p. 415)**

join-prune-interval

- router pim join-prune-interval *< 5 to 65535 >*

  ```
  Usage: join-prune-interval <1-65535>

  Description: Configure interval at which the router will send periodic
               PIM-SM Join/Prune messages. Default is 60 seconds.
  ```

  Range: < 5 to 65535 >

md5-auth-key-chain

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* md5-auth-key-chain

  ```
  Set MD5 authentication method and key chain.
  ```

  Next Available Option:
  - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 413)**

- router ospf area backbone virtual-link *IP-ADDR* md5-auth-key-chain

  ```
  Set MD5 authentication method and key chain.
  ```

  Next Available Option:
  - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 413)**

metric-type

- router ospf area *OSPF-AREA-ID* nssa *< 0 to 16777215 >* metric-type *< type1 | type2 >*

  ```
  Metric type of the type-7 default.
  ```

  Supported Values:
  - **type1** -- Comparable (an OSPF metric plus the external metric).
  - **type2** -- Non-comparable metric (the external metric).
- router ospf area backbone nssa *< 0 to 16777215 >* metric-type *< type1 | type2 >*

  ```
  Metric type of the type-7 default.
  ```

  Supported Values:
  - **type1** -- Comparable (an OSPF metric plus the external metric).
  - **type2** -- Non-comparable metric (the external metric).
- router ospf metric-type *< type1 | type2 >*

  ```
  Usage: metric-type <type1|type2>

  Description: The default metric type used for advertising external routes
               imported into OSPF by this router.
  ```

  Supported Values:
  - **type1** -- Comparable (an OSPF metric plus the external metric).
  - **type2** -- Non-comparable metric (the external metric).

no-advertise

- router ospf area *OSPF-AREA-ID* range no-advertise

```
Do not advertise the range outside the area.
```

- router ospf area backbone range no-advertise

```
Do not advertise the range outside the area.
```

normal

- router ospf area *OSPF-AREA-ID* normal

```
Define a "normal" area.
```

- router ospf area backbone normal

```
Define a "normal" area.
```

no-summary

- router ospf area *OSPF-AREA-ID* nssa *< 0 to 16777215 >* no-summary

```
Do not send summary LSA into the area.
```

- router ospf area *OSPF-AREA-ID* stub no-summary

```
Do not send summary LSA into the area.
```

- router ospf area backbone nssa *< 0 to 16777215 >* no-summary

```
Do not send summary LSA into the area.
```

- router ospf area backbone stub no-summary

```
Do not send summary LSA into the area.
```

nssa

- router ospf area *OSPF-AREA-ID* nssa *< 0 to 16777215 >*

```
Define a "not-so-stubby" area (or NSSA) and its cost.
```

Range: < 0 to 16777215 >

Next Available Options:

- **metric-type** < type1 | type2 > -- Metric type of the type-7 default.**(p. 417)**
- **no-summary** -- Do not send summary LSA into the area.**(p. 418)**

- router ospf area backbone nssa *< 0 to 16777215 >*

```
Define a "not-so-stubby" area (or NSSA) and its cost.
```

Range: < 0 to 16777215 >

Next Available Options:

- **metric-type** < type1 | type2 > -- Metric type of the type-7 default.**(p. 417)**
- **no-summary** -- Do not send summary LSA into the area.**(p. 418)**

ospf

- [no] router ospf

```
Usage: [no] router ospf [...]

Description: Enable/disable/configure Open Shortest Path First (OSPF)
             protocol on the device, or enter OSPF Configuration Context.
             Called without 'no', the command enables OSPF on the device
             and changes current context to OSPF Configuration Context.
             Otherwise ('no' is specified) the command disables OSPF. The
             command can be followed by an OSPF configuration command. Use
             'router ospf ?' to get a list of all possible options.
```

Next Available Options:

- **area** -- Define/remove an OSPF area, area range or virtual link**(p. 410)**
- **default-metric** < 0 to 16777215 > -- The default metric used for advertising external routes imported into OSPF by this router**(p. 414)**
- **distance** -- Set administrative distance to associate with intra-area, inter-area and AS-external routes learned by OSPF**(p. 414)**
- **metric-type** < type1 | type2 > -- The default metric type used for advertising external routes imported into OSPF by this router**(p. 417)**
- **redistribute** < connected | static | rip > -- Specify source protocols which will be redistributed into OSPF**(p. 420)**
- **restrict** -- Prevent redistribution of routes via OSPF**(p. 421)**
- **rfc1583-compatibility** -- Enable/disable RFC-1583 compatibility**(p. 421)**
- **trap** < virtual-interface-state-change | neighbor-state-change | virtual-neighbor-state-change | ... > -- Enable/disable OSPF traps**(p. 425)**

override

- [no] router pim rp-address *IP-ADDR IP-ADDR/MASK-LENGTH* override

```
Specify whether or not static RP configuration precedes the information
learned by a BSR.
```

pim

- [no] router pim

```
Usage: [no] router pim [...]

Description: Enable/disable/configure PIM protocol on the device, or enter
             PIM Configuration Context.
             Called without 'no', the command enables PIM on the device
             and changes current context to PIM Configuration Context.
             Otherwise, the command disables PIM. The command can be
             followed by a PIM configuration command. Use 'router pim ?' to
             get a list of all possible options.
```

Next Available Options:

- **bsr-candidate** -- Configure the router to advertise itself as the Candidate Bootstrap Router (Candidate-BSR) for a PIM-SM domain**(p. 412)**
- **rp-address** -- Statically configure the Rendezvous Point (RP) to accept multicast traffic for specified group or range of groups**(p. 422)**
- **rp-candidate** -- Configure router to advertise itself as the Candidate Rendezvous Point (Candidate-RP) to the Bootstrap Router (BSR)**(p. 423)**

- **join-prune-interval** < 5 to 65535 > -- Configure interval at which the router will send periodic PIM-SM Join/Prune messages**(p. 417)**
- **spt-threshold** -- Specify whether switching to the Shortest Path Tree is enabled or disabled on the router**(p. 424)**
- **state-refresh** < 10 to 300 > -- Set the interval between successive State Refresh messages originated by this router**(p. 424)**
- **trap** < neighbor-loss | hardware-mrt-full | software-mrt-full | ... > -- Enable/disable PIM traps**(p. 425)**

priority

- router pim bsr-candidate priority *< 0 to 255 >*

  ```
  Specify the priority for the Candidate Bootstrap router.
  ```

  Range: < 0 to 255 >
- router pim rp-candidate priority *< 0 to 255 >*

  ```
  Specify the priority for the Candidate-RP router.
  ```

  Range: < 0 to 255 >

range

- [no] router ospf area *OSPF-AREA-ID* range

  ```
  Summarize routes matching address/mask pair.
  ```

  Next Available Options:
  - **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 416)**
  - **no-advertise** -- Do not advertise the range outside the area.**(p. 417)**
  - **type** < summary | nssa > -- Link state database type to apply the range.**(p. 427)**

- [no] router ospf area backbone range

  ```
  Summarize routes matching address/mask pair.
  ```

  Next Available Options:
  - **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 416)**
  - **no-advertise** -- Do not advertise the range outside the area.**(p. 417)**
  - **type** < summary | nssa > -- Link state database type to apply the range.**(p. 427)**

redistribute

- [no] router ospf redistribute *< connected | static | rip >*

  ```
  Usage: [no] redistribute <static|connected|rip>

  Description: Specify source protocols which will be redistributed
               into OSPF.  Use the [no] form of the command to disable
               redistribution of the specified protocol.

      o static    -- redistribute from manually configured routes.
      o connected -- redistribute from locally connected network(s).
      o rip       -- redistribute from RIP routes.
  ```

Supported Values:
- **connected**
- **static**
- **rip**

- [no] router rip redistribute *< connected | static | ospf >*

```
Usage: [no] redistribute <static|connected|ospf>

Description: Specify source protocols which will be redistributed
             into RIP.  Use the [no] form of the command to disable
             redistribution of the specified protocol.

    o static    -- redistribute manually configured routes.
    o connected -- redistribute locally connected network(s).
    o ospf      -- redistribute OSPF routes.
```

Supported Values:
- **connected**
- **static**
- **ospf**

restrict

- router ospf restrict

```
Usage: [no] restrict IP-ADDR/MASK-LEN

Description: Prevent redistribution of routes via OSPF.
```

Next Available Option:
- **ip-addr** -- Prevent redistribution of routes via OSPF (IP-ADDR/MASK-LENGTH) **(p. 416)**

- router rip restrict

```
Usage: [no] restrict IP-ADDR/MASK-LEN

Description: Prevent redistribution of routes via RIP.
```

Next Available Option:
- **ip-addr** -- Prevent redistribution of routes via RIP (IP-ADDR/MASK-LENGTH) **(p. 416)**

retransmit-interval

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- router ospf area backbone virtual-link *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

rfc1583-compatibility

- [no] router ospf rfc1583-compatibility

```
Usage: [no] rfc-1583-compatibility

Description: Enable/disable RFC-1583 compatibility. This controls the
             preference rules used when choosing among multiple
             AS-external-LSAs advertising the same destination. When RFC-1583
             compatibility is disabled, the preference rules are those stated
             in RFC-2328, which prevent routing loops when AS-external-LSAs
             for the same destination have been originated from different
             areas. In order to minimize the chance of routing loops, all OSPF
             routers in an OSPF routing domain should have this parameter to
             be identical. When there are routers present that have not been
             updated with the functionality specified in RFC-2328, all routers
             should have RFC-1583 compatibility enabled. Otherwise, all routers
             should have RFC-1583 compatibility disabled, preventing routing
             loops.
```

rip

- [no] router rip

```
Usage: [no] router rip [...]

Description: Enable/disable/configure Routing Internet Protocol (RIP)
             on the device, or enter RIP Configuration Context.
             Called without 'no', the command enables RIP on the device
             and changes current context to RIP Configuration Context.
             Otherwise, the command disables RIP. The command can be
             followed by a RIP configuration command. Use 'router rip ?' to
             get a list of all possible options.
```

Next Available Options:

- **auto-summary** -- Enable/disable advertisement of summarized routes**(p. 412)**
- **default-metric** < 1 to 15 > -- Set default metric for imported routes**(p. 414)**
- **distance** < 1 to 255 > -- Set administrative distance for routes learned via RIP**(p. 414)**
- **redistribute** < connected | static | ospf > -- Specify source protocols which will be redistributed into RIP**(p. 420)**
- **restrict** -- Prevent redistribution of routes via RIP**(p. 421)**

rp-address

- [no] router pim rp-address

```
Usage: [no] rp-address <IP-ADDR> [GROUP-ADDR/GROUP-MASK] [override]

Description: Statically configure the Rendezvous Point (RP) to accept
             multicast traffic for specified group or range of groups.
             If GROUP-ADDR/GROUP-MASK is not specified, the default multicast
             group prefix 224.0.0.0/4 (224.0.0.0 240.0.0.0) will be used.
             To remove all entries associated with the RP or a specific
             entry use 'no' form of the command.

Parameters:

    o IP-ADDR    - IP address of the Rendezvous Point.
    o GROUP-ADDR - IP address of multicast group, when combined
                   with GROUP-MASK, gives the group prefix.
    o GROUP-MASK - Defines the range of multicast group addresses.
    o override    - Sets the precedence of statically configured RP higher
                    than dynamically learned RPs. Not set by default.
```

Next Available Option:

- **IP-ADDR** -- Specify the IP address of the static RP. (IP-ADDR) **(p. 416)**

rp-candidate

- [no] router pim rp-candidate

```
Usage: rp-candidate [source-ip-vlan <VLAN-ID>]
                    [group-prefix <GROUP-ADDR/GROUP-MASK>]
                    [hold-time <30-255>]
                    [priority <0-255>]
    no rp-candidate [source-ip-vlan <VLAN-ID>]
                    [group-prefix <GROUP-ADDR/GROUP-MASK>]

Description: Configure router to advertise itself as the Candidate
             Rendezvous Point (Candidate-RP) to the Bootstrap Router (BSR).
             When enabling router to be a Candidate-RP the VLAN ID must
             be specified, which IP address will be advertised as a
             Candidate-RP's IP address. PIM-SM must be enabled on the VLAN.
             If GROUP-ADDR/GROUP-MASK is not specified the router will be a
             Candidate-RP for all multicast groups. Use 'no' form of this
             command to remove specific multicast group or disable the router
             to be a Candidate-RP.
             NOTE: It is recommended that the same routing switch is configured
                   as the Candidate-BSR and the Candidate-RP.
Parameters:

    o source-ip-vlan <VLAN-ID> - The VLAN which IP address will be advertised
             as the Candidate-RP address.
    o group-prefix <GROUP-ADDR/GROUP-MASK> - The address and mask that specify
             the multicast group(s) the router uses to advertise in association
             with the Candidate-RP address.
    o hold-time <3-255> - The hold time value (in seconds) to be send to the
             BSR in C-RP-Adv messages. This tells the BSR for how long it
             should consider the sending Candidate-RP router to be operative.
             The default is 150 seconds.
             Note: This value is set to '0' when local system is not a
                   Candidate-RP.
    o priority <0-255> - The priority for the Candidate-RP router for the
             local PIM-SM domain. The smaller value means the higher priority.
             The default is 192.
```

Next Available Options:

- **hold-time** < 30 to 255 > -- Specify the hold time value to be send in C-RP-Adv messages. **(p. 416)**
- **priority** < 0 to 255 > -- Specify the priority for the Candidate-RP router. **(p. 420)**
- **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-RP router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 424)**
- **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 415)**

source-ip-vlan

- [no] router pim bsr-candidate source-ip-vlan *VLAN-ID*

  ```
  Specify the VLAN to use as a source for Candidate-BSR router IP address
  (PIM-SM must be enabled on this VLAN).
  ```

- [no] router pim rp-candidate source-ip-vlan *VLAN-ID*

  ```
  Specify the VLAN to use as a source for Candidate-RP router IP address
  (PIM-SM must be enabled on this VLAN).
  ```

  Next Available Option:

  - **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 415)**

spt-threshold

- [no] router pim spt-threshold

  ```
  Usage: [no] spt-threshold

  Description: Specify whether switching to the Shortest Path Tree is enabled
               or disabled on the router. Default is 'enabled'.
  ```

state-refresh

- router pim state-refresh *< 10 to 300 >*

  ```
  Usage: state-refresh <10-300>

  Description: Set the interval between successive State Refresh messages
               originated by this router. Default value is 60 seconds.
  ```

  Range: < 10 to 300 >

stub

- router ospf area *OSPF-AREA-ID* stub

  ```
  Define a "stub" area and specify its cost.
  ```

  Next Available Options:

  - **cost** < 0 to 16777215 > -- Enter cost to use when injecting default routes into the area.**(p. 413)**
  - **no-summary** -- Do not send summary LSA into the area.**(p. 418)**

- router ospf area backbone stub

  ```
  Define a "stub" area and specify its cost.
  ```

  Next Available Options:

  - **cost** < 0 to 16777215 > -- Enter cost to use when injecting default routes into the area.**(p. 413)**
  - **no-summary** -- Do not send summary LSA into the area.**(p. 418)**

transit-delay

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

- router ospf area backbone virtual-link *IP-ADDR* transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

trap

- [no] router ospf trap *< virtual-interface-state-change | neighbor-state-change | virtual-neighbor-state-change | ... >*

```
Usage: [no] trap <TRAP-NAME|all>

Description: Enable/disable OSPF traps. The traps defined below are generated
             as the result of finding an unusual condition while parsing an
             OSPF packet or a processing a timer event. Note that if more than
             one type of unusual condition is encountered while parsing the
             packet or processing an event, only the first one will generate a
             trap. Possible trap names are:
           - 'interface-state-change' signifies that there has been a change in
             the state of a non-virtual OSPF interface. This trap is generated
             when the interface state regresses (e.g., goes from Dr to Down) or
             progresses to a terminal state (i.e., Point-to-Point, DR Other,
             Dr, or Backup).
           - 'virtual-interface-state-change' signifies the same change in the
             state of a virtual OSPF interface.
           - 'neighbor-state-change' signifies that there has been a change in
             the state of a non-virtual OSPF neighbor. This trap is generated
             when the neighbor state regresses (e.g., goes from Attempt or Full
             to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way
             or Full).
           - 'virtual-neighbor-state-change' signifies the same change in the
             state of a virtual OSPF neighbor.
           - 'interface-config-error' signifies that a packet has been received
             on a non-virtual interface from a router whose configuration
             parameters conflict with this router's configuration parameters.
           - 'virtual-interface-config-error' signifies the same condition on a
             virtual interface.
           - 'interface-authentication-failure' signifies that a packet has
             been received on a non-virtual interface from a router whose
             authentication key or authentication type conflicts with this
             router's authentication key or authentication type.
           - 'virtual-interface-authentication-failure' signifies the same
             condition on a virtual interface.
           - 'interface-receive-bad-packet' signifies that an OSPF packet has
             been received on a non-virtual interface that cannot be parsed.
           - 'virtual-interface-receive-bad-packet' signifies the same
             condition on a virtual interface.
           - 'interface-retransmit-packet' signifies than an OSPF packet has
             been retransmitted on a non-virtual interface.
           - 'virtual-interface-retransmit-packet' signifies the same condition
             on a virtual interface.
           - 'originate-lsa' signifies that a new LSA has been originated by
             this router. This trap is not invoked for simple refreshes of
             LSAs, but instead will only be invoked when an LSA is
             (re)originated due to a topology change. Additionally, this trap
             does not include LSAs that are being flushed because they have
             expired.
           - 'originate-maxage-lsa' signifies that one of the LSA in the
             router's link-state database has expired.
             If 'all' is specified in place of a trap name then all the traps
             are affected by the command.
```

Supported Values:

- **virtual-interface-state-change**
- **neighbor-state-change**
- **virtual-neighbor-state-change**
- **interface-config-error**
- **virtual-interface-config-error**
- **interface-authentication-failure**
- **virtual-interface-authentication-failure**
- **interface-receive-bad-packet**
- **virtual-interface-receive-bad-packet**
- **interface-retransmit-packet**
- **virtual-interface-retransmit-packet**
- **originate-lsa**
- **originate-maxage-lsa**
- **interface-state-change**
- **all**

- [no] router pim trap *< neighbor-loss | hardware-mrt-full | software-mrt-full | ... >*

```
Usage: [no] trap <TRAP-NAME|all>

Description: Enable/disable PIM traps. The traps defined below are generated
             as the result of finding an unusual condition or a timer event.
             Possible trap names are:

           - 'neighbor-loss' signifies that a neighbor timer expired and the
             router has no other neighbors on the same interface with a lower
             IP address than itself.

           - 'hardware-mrt-full' signifies that the MRT table is full and the
             error has been originated by hardware.

           - 'software-mrt-full' signifies that the MRT table is full and the
             error has been originated by software.

             If 'all' is specified in place of a trap name then all the traps
             are affected by the command.
```

Supported Values:

- **neighbor-loss** -- A neighbor router was lost.
- **hardware-mrt-full** -- Hardware MRT table is full.
- **software-mrt-full** -- Software MRT table is full.
- **all** -- All types of traps.

traps

- [no] router vrrp traps

```
Usage: [no] router vrrp traps

Description: Enable/disable generation of VRRP traps. When 'enabled' an
             appropriate SNMP notification message will be sent as a result
             of finding one of the following conditions:
             o 'New Master' - this trap indicates that the sending agent
                              has transitioned to 'Master' state.
             o 'Authentication Failure' - this trap indicates that a packet
                              has been received from a router whose
                              authentication key or authentication type
                              conflicts with this router's authentication
                              key or authentication type.
```

type

- [no] router ospf area *OSPF-AREA-ID* range type < *summary* | *nssa* >

  ```
  Link state database type to apply the range.
  ```

  Supported Values:
  - **summary** -- summary.
  - **nssa** -- nssa.
- [no] router ospf area backbone range type < *summary* | *nssa* >

  ```
  Link state database type to apply the range.
  ```

  Supported Values:
  - **summary** -- summary.
  - **nssa** -- nssa.

virtual-link

- [no] router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR*

  ```
  Specify a virtual neighbor.
  ```

  Next Available Options:
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 424)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 421)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 415)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 414)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 411)**
  - **authentication** -- Disable authentication.**(p. 411)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 417)**

- [no] router ospf area backbone virtual-link *IP-ADDR*

  ```
  Specify a virtual neighbor.
  ```

  Next Available Options:
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 424)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 421)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 415)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 414)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 411)**
  - **authentication** -- Disable authentication.**(p. 411)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 417)**

vrrp

- [no] router vrrp

```
Usage: [no] router vrrp [traps]

Description: Enable/disable/configure Virtual Router Redundancy Protocol (VRRP)
             on the device.
```

Next Available Option:

- **traps** -- Enable/disable generation of VRRP traps**(p. 426)**

r-wireless-services

OVERVIEW

Category:	
Primary context:	config
Related Commands	

COMMAND STRUCTURE

- r-wireless-services **r-wireless-services** -- (SLOT-ID) **(p. 429)**
  - **config** -- (ASCII-STR) **(p. 429)**

COMMAND DETAILS

config (p. 429)	**r-wireless-services (p. 429)**

config

- r-wireless-services *SLOT-ID* config *CONFIG*

r-wireless-services

- r-wireless-services *SLOT-ID*

  Next Available Option:
  - **config** -- (ASCII-STR) **(p. 429)**

setMIB

OVERVIEW

Category:	SNMP
Primary context:	manager
Related Commands	**walkMIB (page 655)**

```
Usage: setmib OBJECT-STR TYPE-STR VALUE-STR
              [[OBJECT-STR TYPE-STR VALUE-STR] ...]

Description: Set the value of a MIB object. The <TYPE-STR> can be:
             -i - integer
             -o - octet
             -d - object identifier
             -a - ip_addr
             -c - counter
             -g - gauge
             -t - time_ticks
             -u - unsigned integer 32
             -D - Display String
             -N - NULL
```

COMMAND STRUCTURE

- setMIB **object** -- MIB object name.instance. (ASCII-STR) **(p. 430)**
  - **type** -- Type of the value to set. See 'setmib help' for details. (ASCII-STR) **(p. 430)**
    - **value** -- A value to which to set the MIB object. (ASCII-STR) **(p. 430)**

COMMAND DETAILS

object (p. 430)	**type (p. 430)**	**value (p. 430)**

object

- setMIB *OBJECT*

```
MIB object name.instance.
```

Next Available Option:

- **type** -- Type of the value to set. See 'setmib help' for details. (ASCII-STR) **(p. 430)**

type

- setMIB *OBJECT TYPE*

```
Type of the value to set. See 'setmib help' for details.
```

Next Available Option:

- **value** -- A value to which to set the MIB object. (ASCII-STR) **(p. 430)**

value

- setMIB *OBJECT TYPE VALUE*

```
A value to which to set the MIB object.
```

setup

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	

```
Usage: setup [default-logon <CLI|Menu>]

Description: Enter the 'Switch Setup' screen for basic switch configuration.
             The optional parameter 'default-logon' changes the user
             interface presented after boot without entering full-screen
             setup.
```

COMMAND STRUCTURE

- setup **default-logon < CLI | Menu >** -- Specify whether switch should boot to CLI (default) or menu. **(p. 433)**

EXAMPLES

Example: setup

Access the Switch Setup screen to quickly configure IP addressing and other basic settings:

```
ProCurve# setup
ProCurve                                                    1-Jan-2001   2:14:27
===========================- TELNET - MANAGER MODE -============================
                                  Switch Setup

  System Name : HPswitch
  System Contact : Sysadmin
  Manager Password : ***********        Confirm Password : ***********
  Logon Default : CLI                   Time Zone [0] : -480
  Community Name : public               Spanning Tree Enabled [No] : No

  Default Gateway : 10.10.10.1
  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled

  IP Config [DHCP/Bootp] : Manual
  IP Address  : 10.10.10.150
  Subnet Mask : 255.255.255.0


 Actions->   Cancel     Edit     Save     Help

Enter System Name - up to 25 characters.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

COMMAND DETAILS

default-logon (p. 433)

default-logon

- setup default-logon *< CLI | Menu >*

```
Specify whether switch should boot to CLI (default) or menu.
```

Supported Values:

- **CLI** -- Set Command Line Interface as default console interface.
- **Menu** -- Set Menu as default console interface.

sflow

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: sflow <RECEIVER-INSTANCE> destination <IP-ADDRESS> [UDP-PORT]
       sflow <RECEIVER-INSTANCE> polling [ethernet] PORT-LIST
             <POLLING-INTERVAL>
       sflow <RECEIVER-INSTANCE> sampling [ethernet] PORT-LIST
             <SAMPLING-RATE>
       [no] sflow <RECEIVER-INSTANCE>

Description: Configure or un-claim an sflow sampling receiver.
             If the [no] option is not used, this command will
             configure the sflow sampling receiver, polling,
             and sampling.

Parameters:  IP-ADDRESS - Ip address of the sFlow
             receiver/collector/management station

             UDP-PORT - The udp application port of the sFlow
             receiver/collector/management station (default: 6343).

             POLLING-INTERVAL - The maximum interval (seconds) between
             polling of counters. (a value of 0 causes polling to be
             disabled.

             PORT-LIST - Port(s) for which packet are to be sampled.

             RECEIVER-INSTANCE - One of three posible sFlow receiver tables.

             SAMPLING-RATE - N, where 1/N is the number of packets sampled.
             (a value of 0 causes sampling to be disabled.)
```

COMMAND STRUCTURE

- [no] sflow **sflow-receiver** **< 1 to 3 >** -- Select one of three possible sFlow receiver tables. (NUMBER) **(p. 436)**
  - **destination** -- IP address of sFlow receiver/collector/management station. (IP-ADDR) **(p. 435)**
    - **sflow-udp-port** **< 1 to 65535 >** -- UDP application port of sFlow receiver/collector/management station. (NUMBER) **(p. 436)**
  - **polling** -- Specify the ports for which packets are to be polled. ([ethernet] PORT-LIST) **(p. 435)**
    - **sflow-polling-interval** **< 20 to 16777215 >** -- Specify the maximum interval (seconds) between polling of counters. **(p. 435)**
    - **sflow-polling-int-off** **< 0 >** -- Disable polling of counters. **(p. 435)**
  - **sampling** -- Specify the ports for which packets are to be sampled. ([ethernet] PORT-LIST) **(p. 435)**
    - **sflow-sampler-off** **< 0 >** -- Disable sampling. **(p. 436)**
    - **sflow-sampler-rate** **< 50 to 16441700 >** -- Specify N, where 1/N is the number of packets sampled. **(p. 436)**

COMMAND DETAILS

destination

- sflow *< 1 to 3 >* destination *IP-ADDR*

```
IP address of sFlow receiver/collector/management station.
```

Next Available Option:

- **sflow-udp-port** < 1 to 65535 > -- UDP application port of sFlow receiver/collector/management station. (NUMBER) **(p. 436)**

polling

- sflow *< 1 to 3 >* polling *[ETHERNET] PORT-LIST*

```
Specify the ports for which packets are to be polled.
```

Next Available Options:

- **sflow-polling-int-off** < 0 > -- Disable polling of counters. **(p. 435)**
- **sflow-polling-interval** < 20 to 16777215 > -- Specify the maximum interval (seconds) between polling of counters. **(p. 435)**

sampling

- sflow *< 1 to 3 >* sampling *[ETHERNET] PORT-LIST*

```
Specify the ports for which packets are to be sampled.
```

Next Available Options:

- **sflow-sampler-off** < 0 > -- Disable sampling. **(p. 436)**
- **sflow-sampler-rate** < 50 to 16441700 > -- Specify N, where 1/N is the number of packets sampled. **(p. 436)**

sflow-polling-interval

- sflow *< 1 to 3 >* polling *[ETHERNET] PORT-LIST < 20 to 16777215 >*

```
Specify the maximum interval (seconds) between polling of counters.
```

Range: < 20 to 16777215 >

sflow-polling-int-off

- sflow *< 1 to 3 >* polling *[ETHERNET] PORT-LIST < 0 >*

```
Disable polling of counters.
```

Supported Values:

- **0** -- Disable polling.

sflow-receiver

- [no] sflow *< 1 to 3 >*

  ```
  Select one of three possible sFlow receiver tables.
  ```

  Range: < 1 to 3 >

  Next Available Options:

  - **destination** -- IP address of sFlow receiver/collector/management station. (IP-ADDR) **(p. 435)**
  - **polling** -- Specify the ports for which packets are to be polled. ([ethernet] PORT-LIST) **(p. 435)**
  - **sampling** -- Specify the ports for which packets are to be sampled. ([ethernet] PORT-LIST) **(p. 435)**

sflow-sampler-off

- sflow *< 1 to 3 >* sampling *[ETHERNET] PORT-LIST < 0 >*

  ```
  Disable sampling.
  ```

  Supported Values:

  - **0** -- Disable sampling.

sflow-sampler-rate

- sflow *< 1 to 3 >* sampling *[ETHERNET] PORT-LIST < 50 to 16441700 >*

  ```
  Specify N, where 1/N is the number of packets sampled.
  ```

  Range: < 50 to 16441700 >

sflow-udp-port

- sflow *< 1 to 3 >* destination *IP-ADDR < 1 to 65535 >*

  ```
  UDP application port of sFlow receiver/collector/management station.
  ```

  Range: < 1 to 65535 >

show

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: show ...

Description: Display switch operation information.
             The 'show' must be followed by a command.
             Use 'show ?' for the list of all possible command.
```

COMMAND STRUCTURE

- show **access-list** -- Show Access Control List information **(p. 451)**
  - **acl-name** -- Display detailed information on specified ACL. (ASCII-STR) **(p. 452)**
    - **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 462)**
  - **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 462)**
  - **ports** -- Show ACLs applied to the specified ports. ([ethernet] PORT-LIST) **(p. 498)**
  - **radius** -- Display ACLs applied via RADIUS. ([ethernet] PORT-LIST) **(p. 500)**
  - **resources** -- Display ACL Rules/Masks availability. **(p. 502)**
  - **vlan** -- Show ACLs applied to the specified VLAN. (VLAN-ID) **(p. 518)**
- show **accounting** -- Show Accounting configuration parameters **(p. 452)**
  - **sessions** -- Show accounting data for all active sessions **(p. 507)**
- show **arp** -- Show the IP ARP translation table **(p. 454)**
  - **vlan** -- Specify VLAN for which to show ARP entries. (VLAN-ID) **(p. 518)**
- show **arp-protect** -- Display Dynamic ARP Protection information **(p. 454)**
  - **statistics** -- (VLAN-ID-RANGE) **(p. 510)**
- show **authentication** -- Show Authentication configuration parameters **(p. 454)**
- show **authorization** -- Show Authorization configuration parameters **(p. 455)**
- show **autorun** -- Show Autorun configuration status. **(p. 456)**
- show **bandwidth** -- Show queue percentages for outbound guaranteed minimum bandwidth **(p. 457)**
  - **output** -- Show outbound guaranteed minimum bandwidth. **(p. 494)**
    - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**
- show **banner** -- show the configured banner text **(p. 457)**
  - **motd** -- show the configured banner text **(p. 490)**
- show **boot-history** -- Display the system boot log **(p. 458)**
- show **cdp** -- Show CDP configuration and neighbors discovered **(p. 459)**
  - **neighbors** -- Show CDP neighbors. See 'show cdp help' for details. **(p. 492)**
    - **detail** -- Show neighbor information field-per-line instead of shortened table format. **(p. 467)**
    - **neighbors-port** -- Show CDP neighbors on specified port only. ([ethernet] PORT-NUM) **(p. 493)**
- show **config** -- Show the switch startup configuration **(p. 462)**
  - **filename < config | new >** -- Display specified configuration. **(p. 471)**
  - **files** -- List saved configuration files. **(p. 471)**
  - **status** -- Check if the running configuration differs from the statup configuration. **(p. 511)**

- show **connection-rate-filter** -- List the ports and the on/off connection-rate-filter status and sensitivity **(p. 465)**
  - **all-hosts** -- Show blocked and throttled IP addresses. **(p. 453)**
  - **blocked-hosts** -- Show blocked IP addresses. **(p. 458)**
  - **throttled-hosts** -- Show throttled IP addresses. **(p. 514)**
- show **console** -- Show serial link/console settings **(p. 465)**
- show **cpu** -- Show average CPU utilization over the last 1, 5, and 60 seconds; or the number of seconds specified **(p. 465)**
  - **slot** -- Display module CPU statistics. (SLOT-ID-RANGE) **(p. 507)**
    - **slave_time < 1 to 90 >** -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 507)**
  - **time < 1 to 300 >** -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 514)**
- show **crypto** -- Display flash files used for authentication **(p. 466)**
  - **autorun-cert** -- Display trusted certificate. **(p. 456)**
  - **autorun-key** -- Display autorun key. **(p. 456)**
  - **client-public-key** -- Display ssh authorized client public keys. **(p. 459)**
    - **babble** -- Display phonetic hash. **(p. 457)**
    - **fingerprint** -- Display hexadecimal hash. **(p. 472)**
    - **keyfile < manager | operator >** -- Choose to display manager or operator keys. **(p. 484)**
      - **babble** -- Display phonetic hash. **(p. 457)**
      - **fingerprint** -- Display hexadecimal hash. **(p. 472)**
      - **keylist** -- Select keys to display (comma-delimited list). (ASCII-STR) **(p. 484)**
        - **babble** -- Display phonetic hash. **(p. 457)**
        - **fingerprint** -- Display hexadecimal hash. **(p. 472)**
  - **host-cert** -- Display https certificate information. **(p. 475)**
  - **host-public-key** -- Display ssh host RSA public key. **(p. 475)**
    - **babble** -- Display phonetic hash. **(p. 457)**
    - **fingerprint** -- Display hexadecimal hash. **(p. 472)**
- show **debug** -- Display currently active debug log destinations and types **(p. 466)**
  - **buffer** -- Show the contents of the debug log buffer. **(p. 459)**
- show **dhcp-relay** -- Shows the current status of DHCP Relay Agent and option 82 statistics **(p. 469)**
- show **dhcp-snooping** -- Display DHCP snooping information **(p. 469)**
  - **binding** -- Display DHCP snooping binding information. **(p. 457)**
  - **stats** -- Display DHCP snooping events. **(p. 511)**
- show **fastboot** -- Shows the current status of fastboot on switch **(p. 471)**
- show **fault-finder** -- Show the fault-finder table **(p. 471)**
- show **filter** -- Show a table of security filters or a filter detailed information, if the filter's INDEX is specified **(p. 472)**
  - **INDEX** -- Show detailed information for the filter identified by the INDEX. The indices are displayed by the 'show filter' command. **(p. 477)**
  - **source-port** -- **(p. 508)**
- show **flash** -- Show the version of software stored in the Primary and Secondary image locations **(p. 472)**
- show **front-panel-security** -- Show current security status of the front panel butons **(p. 473)**
- show **gvrp** -- Show GVRP settings **(p. 474)**
- show **history** -- Show previously entered commands **(p. 475)**
- show **igmp** -- Show global switch IGMP configuration parameters **(p. 476)**
  - **delayed-flush** -- Shows switch-wide IGMP delayed flush value **(p. 467)**
- show **igmp-proxy** -- Show active/configured IGMP proxy forwarder information **(p. 477)**
  - **domains** -- Show all the currently configured IGMP proxy domains. **(p. 469)**
  - **entries** -- Show all the currently active IGMP proxy entries. **(p. 470)**
  - **vlans** -- Show all the VLANs currently associated with IGMP proxy domains. **(p. 521)**
- show **instrumentation** -- Show internal version-dependant counters for debugging **(p. 478)**

  - **monitor** -- Show latest values for monitored parameters **(p. 489)**
    - **configuration** -- show configured thresholds for monitored parameters **(p. 465)**
- show **interfaces** -- Show port configuration and status information **(p. 480)**
  - **brief** -- Show the ports' operational parameters **(p. 458)**
    - **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 496)**
  - **config** -- Show configuration information **(p. 462)**
  - **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 496)**
    - **hc** -- Show summary of network traffic handled by the ports **(p. 474)**
  - **port-utilization** -- Show the ports' bandwidth-utilization **(p. 498)**
- show **ip** -- Show the device IP configuration **(p. 480)**
  - **authorized-managers** -- Show IPV4 addresses allowed to manage the switch **(p. 455)**
  - **client-public-key** -- Show currently loaded public keys for authorized clients (NUMBER) **(p. 459)**
    - **babble** -- Display phonetic hash. **(p. 457)**
    - **fingerprint** -- Display hexadecimal hash. **(p. 472)**
  - **dns** -- Show configured DNS server IP addresses on the switch **(p. 469)**
  - **forward-protocol** -- Show server addresses where broadcast requests received by the switch are to be forwarded based on configured port **(p. 472)**
    - **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 518)**
  - **helper-address** -- Show DHCP servers where DHCP requests received by the switch are to be forwarded **(p. 475)**
    - **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 518)**
  - **host-public-key** -- Display the SSH host RSA public key (NUMBER) **(p. 475)**
    - **babble** -- Display phonetic hash. **(p. 457)**
    - **fingerprint** -- Display hexadecimal hash. **(p. 472)**
  - **icmp** -- Show ICMP Rate Limiting settings **(p. 476)**
  - **igmp** -- Invoked without any parameters, shows per-VLAN IGMP status, or, if VLANs are disabled displays the global IGMP status **(p. 476)**
    - **config** -- Show IGMP configuration information. **(p. 462)**
    - **group** -- Show ports the specified multicast group address is registered on. (IP-ADDR) **(p. 473)**
    - **vlan** -- Show IGMP operational information for the VLAN specified. (VLAN-ID) **(p. 518)**
      - **config** -- Show IGMP configuration information for the VLAN specified. **(p. 462)**
  - **irdp** -- Show IRDP (ICMP Router Discovery Protocol) settings **(p. 483)**
  - **mroute** -- Show IP multicast routing table **(p. 490)**
    - **interface** -- Show IP multicast routing interfaces' information **(p. 479)**
      - **VLAN-ID** -- Specify the VLAN ID of the IP multicast routing interface to show. (VLAN-ID) **(p. 520)**
    - **IP-ADDR** -- Show detailed information for the specified entry from the IP multicast routing table (IP-ADDR) **(p. 481)**
      - **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 481)**
  - **ospf** -- Show OSPF operational and configuration information **(p. 493)**
    - **area** -- Show OSPF areas configured on the device **(p. 453)**
      - **area-ip** -- (OSPF-AREA-ID) **(p. 454)**
    - **external-link-state** -- Show the Link State Advertisements from throughout the areas to which the device is attached **(p. 471)**
      - **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation. **(p. 452)**
      - **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 485)**
      - **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 505)**
      - **sequence-number** -- Show LSAs with the specified sequence number only. **(p. 506)**
      - **status** -- The keyword is optional and can be omitted. **(p. 511)**
    - **general** -- Show OSPF basic configuration and operational information **(p. 473)**

        - **interface** -- Show OSPF interfaces' information **(p. 479)**
            - **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 476)**
            - **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 518)**
        - **link-state** -- Show all Link State Advertisements from throughout the areas to which the device is attached **(p. 485)**
            - **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation. **(p. 452)**
            - **area-id** -- Show LSAs for the specified area only. (OSPF-AREA-ID) **(p. 454)**
            - **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 485)**
            - **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 505)**
            - **sequence-number** -- Show LSAs with the specified sequence number only. **(p. 506)**
            - **status** -- The keyword is optional and can be omitted. **(p. 511)**
            - **type < router | network | summary | ... >** -- Show LSAs of the specified type only. **(p. 515)**
        - **neighbor** -- Show all OSPF neighbors in the locality of of the device **(p. 492)**
            - **neighbor-ip** -- (IP-ADDR) **(p. 492)**
        - **redistribute** -- List protocols which are being redistributed into OSPF **(p. 501)**
        - **restrict** -- List routes which will not be redistributed via OSPF **(p. 503)**
        - **traps** -- Show OSPF traps enabled on the device **(p. 515)**
        - **virtual-link** -- Show status of all OSPF virtual links configured **(p. 517)**
            - **area** -- Specify area of the virtual links to show. (OSPF-AREA-ID) **(p. 453)**
            - **vlink-ip** -- Router ID of the link destination for which to show detailed information. (IP-ADDR) **(p. 521)**
        - **virtual-neighbor** -- Show all virtual neighbors of the device **(p. 518)**
            - **area** -- Specify area of the virtual neighbors to show. (OSPF-AREA-ID) **(p. 453)**
            - **vneighbor-ip** -- Router ID of the virtual neighbor for which to show detailed information. (IP-ADDR) **(p. 521)**
    - **pim** -- Show PIM protocol operational and configuration information **(p. 495)**
        - **bsr** -- Show Bootstrap Router information **(p. 458)**
            - **elected** -- Show elected Bootstrap Router information. **(p. 470)**
            - **local** -- Show local Candidate-BSR configuration information. **(p. 486)**
        - **interface** -- Show PIM interface information **(p. 479)**
            - **VLAN-ID** -- Specify the VLAN ID of the PIM interface to show. (VLAN-ID) **(p. 520)**
        - **mroute** -- Show PIM-specific information from the IP multicast routing table **(p. 490)**
            - **IP-ADDR** -- Specify the IP multicast group address of the MRT entry. (IP-ADDR) **(p. 481)**
                - **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 481)**
        - **neighbor** -- Show PIM neighbor information **(p. 492)**
            - **IP-ADDR** -- Specify the IP address of the PIM neighbor to show. (IP-ADDR) **(p. 481)**
        - **pending** -- Show (*,G) and (S,G) Join Pending Information. **(p. 495)**
        - **rp-candidate** -- Show Candidate-RP operational and configuration information **(p. 505)**
            - **config** -- Show C-RP configuration information. **(p. 462)**
        - **rp-pending** -- Show (*,*,RP) Join Pending Information. **(p. 505)**
        - **rp-set** -- Show RP-Set information available on the router **(p. 505)**
            - **learned** -- Show RP-Set information learned from the BSR. **(p. 484)**
            - **static** -- Show statically configured RP-Set information. **(p. 510)**
    - **rip** -- Show RIP operational and configuration information **(p. 503)**
        - **general** -- Show RIP basic configuration and operational information **(p. 473)**
        - **interface** -- Show RIP interfaces' information **(p. 479)**
            - **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 476)**
            - **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 518)**

    - **peer** -- Show RIP peers **(p. 494)**
      - **peer-ip** -- Specify IP address of the RIP peer to show. (IP-ADDR) **(p. 494)**
    - **redistribute** -- List protocols which are being redistributed into RIP **(p. 501)**
    - **restrict** -- List routes which will not be redistributed via RIP **(p. 503)**
  - **route** -- Show the IP routing table **(p. 504)**
    - **ip-addr** -- Destination IP address to display the routes to. (IP-ADDR) **(p. 481)**
    - **type < static | connected | rip | ... >** -- Specify type of routes to display. **(p. 515)**
  - **ssh** -- Show both current SSH configuration and the status of active connections **(p. 509)**
- show **ip-recv-mac-address** -- Show VLAN L3-Mac-Address table. **(p. 482)**
- show **ipv6** -- Show the device IPv6 configuration **(p. 482)**
  - **authorized-managers** -- Show IPV6 addresses allowed to manage the switch **(p. 455)**
  - **mld** -- Invoked without any parameters, shows per-VLAN MLD status, or, if VLANs are disabled displays the global MLD status **(p. 489)**
    - **config** -- Show MLD configuration information. **(p. 462)**
    - **statistics** -- Show MLD statistics. **(p. 510)**
    - **vlan** -- Show MLD VLAN information. **(p. 518)**
      - **vlan-id** -- Show MLD operational information for the VLAN specified. (VLAN-ID) **(p. 520)**
        - **config** -- Show MLD configuration information for the VLAN specified. **(p. 462)**
        - **counters** -- Show MLD VLAN counter information. **(p. 465)**
        - **group** -- Show MLD VLAN group info. **(p. 473)**
          - **ipv6-addr** -- Show MLD VLAN group address information. (IPV6-ADDR) **(p. 482)**
        - **statistics** -- Show MLD VLAN statistics **(p. 510)**
  - **neighbors** -- Displays information on the IPv6 neighbor discovery cache **(p. 492)**
    - **vlan** -- Displays information on the IPv6 neighbor discovery cache **(p. 518)**
      - **vlan** -- Show IPv6 information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**
  - **route** -- Show the IPv6 routing table **(p. 504)**
    - **ipv6-addr** -- Destination IPv6 address to display the routes to. (IPV6-ADDR) **(p. 482)**
    - **type < connected >** -- Specify type of routes to display. **(p. 515)**
  - **routers** -- Show the IPv6 Router table entries **(p. 505)**
    - **vlan** -- Show the IPv6 Router Table Entries for VLAN. **(p. 518)**
      - **vlan** -- Show IPv6 information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**
  - **vlan** -- Show IPv6 status information for all VLANs **(p. 518)**
    - **vlan** -- Show IPv6 information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**
- show **jumbos** -- Show the untagged Max frame size for the switch **(p. 483)**
- show **key-chain** -- Display key chains **(p. 483)**
  - **CHAIN-NAME** -- Show the chain detailed information. (ASCII-STR) **(p. 459)**
- show **lacp** -- Show status of LACP trunks **(p. 484)**
- show **licenses** -- Display license status for premium features **(p. 484)**
  - **uninstalled** -- Display verification key for features which have been uninstalled. **(p. 516)**
- show **link-keepalive** -- show link-keepalive information on the switch **(p. 485)**
  - **statistics** -- show detailed statistics for all link-keepalive enabled ports. **(p. 510)**
- show **lldp** -- Show various LLDP settings **(p. 485)**
  - **auto-provision** -- Show LLDP auto-provision related info for radio-ports **(p. 456)**
    - **radio-ports** -- Show LLDP radio-ports information. **(p. 500)**
  - **config** -- Show LLDP configuration information **(p. 462)**
    - **port-list** -- Specify the port or list of ports. ([ethernet] PORT-LIST) **(p. 496)**
  - **info** -- Show LLDP information about the remote or local device **(p. 477)**
    - **local-device** -- Show LLDP local device information. **(p. 486)**
      - **port-list** -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) **(p. 496)**
    - **remote-device** -- Show LLDP remote device information. **(p. 502)**
      - **port-list** -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) **(p. 496)**

  - **stats** -- Show LLDP statistics **(p. 511)**
    - **port-list** -- Specify the port or list of ports. ([ethernet] PORT-LIST) **(p. 496)**
- show **lockout-mac** -- Show the MAC addresses that have been locked out of the network **(p. 486)**
- show **logging** -- Display log events **(p. 486)**
  - **-a** -- Display all log events, including those from previous boot cycles. **(p. 451)**
  - **event_class** **< -M | -P | -W | ... >** -- Specify substring to match in log entry. See 'log help' for details. **(p. 470)**
  - **option** -- Filter events shown. See 'show logging help' for details. (ASCII-STR) **(p. 493)**
  - **-r** -- Display log events in reverse order (most recent first). **(p. 500)**
- show **loop-protect** -- Show loop protection status **(p. 487)**
  - **port-list** -- Show loop protection summary for ports. ([ethernet] PORT-LIST) **(p. 496)**
- show **mac-address** -- Show MAC addresses the switch has learned **(p. 487)**
  - **address-table-port** -- Show MAC addresses learned on the specified ports. ([ethernet] PORT-LIST) **(p. 452)**
  - **MAC** -- Show port the specified MAC address is located on. (MAC-ADDR) **(p. 487)**
  - **vlan** -- Show MAC addresses learned on the specified VLAN. (VLAN-ID) **(p. 518)**
- show **management** -- Show the switch's addresses available for management and the time server if the switch uses one **(p. 488)**
- show **mesh** -- Show the switch mesh information such as mesh ports, adjacent switches and their peer ports **(p. 488)**
- show **modules** -- **(p. 489)**
- show **monitor** -- Show the switch network monitoring status and configuration, if network monitoring is enabled **(p. 489)**
  - **endpoint** -- Remote mirroring destination configuration. **(p. 470)**
  - **mirror_session_id** **< 1 to 4 >** -- Mirror destination number. **(p. 489)**
  - **name** -- Mirror destination name. **(p. 492)**
- show **name** -- Show names assigned to the ports **(p. 492)**
  - **port-list** -- Show names assigned to the ports ([ethernet] PORT-LIST) **(p. 496)**
- show **port-access** -- Show 802.1x supplicant or authenticator statistics and configuration. **(p. 495)**
  - -- Show Web/MAC Authentication statistics and configuration ([ethernet] PORT-LIST) **(p. 449)**
    - **authenticator** -- Show 802.1X authenticator statistics and configuration. **(p. 455)**
      - **clients** -- Show the current 802.1X client session statistics. **(p. 460)**
        - **detailed** -- Show the current 802.1X client session detailed statistics. **(p. 468)**
      - **config** -- Show 802.1X authenticator configuration. **(p. 462)**
      - **session-counters** -- Show 802.1X current (or last if no current sessions open) sessions counters. **(p. 506)**
      - **statistics** -- Show authentication sessions statistics for 802.1X authenticator. **(p. 510)**
      - **vlan** -- Show authorized and unauthorized vlans for 802.1X authenticator. **(p. 518)**
    - **mac-based** -- Show MAC Authentication statistics and configuration **(p. 487)**
      - **clients** -- Show the connected MAC address information. **(p. 460)**
        - **detailed** -- Show the connected MAC address detailed information. **(p. 468)**
      - **config** -- Show the current configuration of MAC Authentication. **(p. 462)**
        - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
        - **detailed** -- Show the detailed configuration of MAC Authentication. **(p. 468)**
    - **web-based** -- Show Web Authentication statistics and configuration **(p. 522)**
      - **clients** -- Show the current web client session statistics. **(p. 460)**
        - **detailed** -- Show the current web client session detailed statistics. **(p. 468)**
      - **config** -- Show the current configuration of Web Authentication. **(p. 462)**
        - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
        - **detailed** -- Show the detailed configuration of Web Authentication. **(p. 468)**
        - **web-server** -- Show the web server-related configuration items. **(p. 523)**
  - **authenticator** -- Show 802.1X statistics and configuration. **(p. 455)**
    - -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 449)**

    - **clients** -- Show the current 802.1X client session statistics. **(p. 460)**
      - **detailed** -- Show the current 802.1X client session detailed statistics. **(p. 468)**
    - **config** -- Show 802.1X authenticator configuration. **(p. 462)**
    - **session-counters** -- Show 802.1X current (or last if no current sessions open) sessions counters. **(p. 506)**
    - **statistics** -- Show authentication sessions statistics for 802.1X authenticator. **(p. 510)**
    - **vlan** -- Show authorized and unauthorized vlans for 802.1X authenticator. **(p. 518)**
  - **clients** -- Show the current 802.1X client session statistics. **(p. 460)**
    - -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 449)**
      - **detailed** -- Show the current 802.1X client session detailed statistics. **(p. 468)**
  - **config** -- Show 802.1X authenticator configuration. **(p. 462)**
  - **session-counters** -- Show 802.1X current (or last if no current sessions open) sessions counters. **(p. 506)**
  - **statistics** -- Show authentication sessions statistics for 802.1X authenticator. **(p. 510)**
  - **vlan** -- Show authorized and unauthorized vlans for 802.1X authenticator. **(p. 518)**
- **config** -- Show status of 802.1X, Web Auth, and MAC Auth configurations. **(p. 462)**
- **mac-based** -- Show MAC Authentication statistics and configuration **(p. 487)**
  - -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
    - **clients** -- Show the connected MAC address information. **(p. 460)**
      - **detailed** -- Show the connected MAC address detailed information. **(p. 468)**
    - **config** -- Show the current configuration of MAC Authentication. **(p. 462)**
      - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
      - **detailed** -- Show the detailed configuration of MAC Authentication. **(p. 468)**
  - **clients** -- Show the connected MAC address information. **(p. 460)**
    - -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
      - **detailed** -- Show the connected MAC address detailed information. **(p. 468)**
  - **config** -- Show the current configuration of MAC Authentication. **(p. 462)**
    - -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
      - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
      - **detailed** -- Show the detailed configuration of MAC Authentication. **(p. 468)**
    - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
- **supplicant** -- Show 802.1X port-access supplicant statistics. **(p. 512)**
  - -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 449)**
  - **statistics** -- Show authentication sessions statistics for 802.1X supplicant. **(p. 510)**
- **web-based** -- Show Web Authentication statistics and configuration **(p. 522)**
  - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
    - **clients** -- Show the current web client session statistics. **(p. 460)**
      - **detailed** -- Show the current web client session detailed statistics. **(p. 468)**
    - **config** -- Show the current configuration of Web Authentication. **(p. 462)**
      - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
      - **detailed** -- Show the detailed configuration of Web Authentication. **(p. 468)**
      - **web-server** -- Show the web server-related configuration items. **(p. 523)**
  - **clients** -- Show the current web client session statistics. **(p. 460)**
    - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
      - **detailed** -- Show the current web client session detailed statistics. **(p. 468)**
  - **config** -- Show the current configuration of Web Authentication. **(p. 462)**
    - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**

        - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
        - **detailed** -- Show the detailed configuration of Web Authentication. **(p. 468)**
        - **web-server** -- Show the web server-related configuration items. **(p. 523)**
      - **auth-server** -- Show the authentication server-related configuration items. **(p. 456)**
      - **web-server** -- Show the web server-related configuration items. **(p. 523)**
- show **port-security** -- Show a table describing port security settings **(p. 498)**
  - **intrusion-log** -- Show the intrusion log records. **(p. 480)**
  - **port-list** -- Show a table describing port security settings ([ethernet] PORT-LIST) **(p. 496)**
- show **power-over-ethernet** -- Show port poe configuration and status information **(p. 499)**
  - **brief** -- Show summary of poe status **(p. 458)**
    - **port-list** -- Show the ports' poe status ([ethernet] PORT-LIST) **(p. 496)**
    - **slot** -- Show summary of poe status (SLOT-ID-RANGE) **(p. 507)**
  - **port-list** -- Show the ports' poe status ([ethernet] PORT-LIST) **(p. 496)**
  - **slot** -- Show poe information of specified slot (SLOT-ID-RANGE) **(p. 507)**
- show **qinq** -- show qinq configuration details **(p. 500)**
- show **qos** -- Show various QoS settings **(p. 500)**
  - **device-priority** -- Show the device priority table (priority based on the IP addresses) **(p. 469)**
  - **dscp-map** -- Show mappings between DSCP policy and 802.1p priority. **(p. 470)**
  - **port-priority** -- Show the port-based priority table **(p. 497)**
  - **protocol-priority** -- Show the protocol priority **(p. 499)**
  - **queue-config** -- Displays outbound port queues configuration information. **(p. 500)**
  - **resources** -- Show the qos resources **(p. 502)**
  - **tcp-udp-port-priority** -- Show TCP/UDP port priorities **(p. 513)**
  - **type-of-service** -- Show QoS priorities based on IP Type-of-Service **(p. 516)**
  - **vlan-priority** -- Show the VLAN-based priority table **(p. 521)**
- show **radius** -- Show RADIUS status and statistics information **(p. 500)**
  - **accounting** -- Show RADIUS accounting statistics **(p. 452)**
  - **authentication** -- Show RADIUS authentication statistics **(p. 454)**
  - **dyn-authorization** -- Show RADIUS dynamic authorization statistics **(p. 470)**
  - **host** -- Show statistics information for the RADIUS host (IP-ADDR) **(p. 475)**
    - **dyn-authorization** -- **(p. 470)**
- show **rate-limit** -- Show rate limit maximum percentages **(p. 501)**
  - **all** -- Show limits for all traffic. **(p. 453)**
    - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**
  - **icmp** -- Show only limits for icmp traffic. **(p. 476)**
    - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**
  - **ip** -- ip help **(p. 480)**
    - **access-group** -- access-group **(p. 451)**
      - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**
- show **redundancy** -- Display redundant information for Management and Fabric Modules **(p. 502)**
- show **rmon** -- Show detailed rmon statistics for the ports **(p. 503)**
  - **statistics** -- Show RMON statistics for the ports ([ethernet] PORT-LIST) **(p. 510)**
- show **running-config** -- Show the switch running configuration **(p. 506)**
  - **status** -- Check if the running configuration differs from the statup configuration. **(p. 511)**
- show **sflow** -- Display information regarding the configuration, sampling, and polling with respect to 'sflow' **(p. 507)**
  - **agent** -- Displays read-only switch agent information: The agent address is normally the ip address of the first vlan configured. **(p. 453)**
  - **receiver-index** **< 1 to 3 >** -- Select one of the three possible sFlow receiver tables. (NUMBER) **(p. 501)**

- **destination** -- Displays information about the receiver/collector/management-station to which the sampling-polling data is sent. **(p. 467)**
- **sampling-polling** -- Displays information about sampling and polling. **(p. 506)**
    - **port-list** -- Displays information about sampling and polling. ([ethernet] PORT-LIST) **(p. 496)**
- show **snmp-server** -- Display information on all SNMP communities, trap receivers and Snmp response/trap source-ip policy configured on the switch **(p. 508)**
    - **community** -- Specify SNMP community to which to restrict the output. (ASCII-STR) **(p. 461)**
    - **traps** -- Show all configured traps. **(p. 515)**
- show **snmpv3** -- Show configuration of SNMPv3 features. **(p. 508)**
    - **access-rights** -- Show information about access rights. **(p. 452)**
        - **group < ManagerPriv | ManagerAuth | OperatorAuth | ... >** -- Show SNMPv3 users. **(p. 473)**
            - **sec-model** -- Set security model. **(p. 506)**
                - **ver1-2c < ver1 | ver2c >** -- Configure SNMPv3 User entry. **(p. 516)**
                - **ver3** -- SNMP version 3 security model. **(p. 517)**
                    - **ver3 < noauth | auth | priv >** -- Set security level. **(p. 517)**
    - **community** -- Show SNMPv3 Community table. **(p. 461)**
        - **COMMUNITY-NAME** -- Show a specific community entry. (ASCII-STR) **(p. 461)**
    - **enable** -- Show SNMPv3 status. **(p. 470)**
    - **engineid** -- Show switch's SNMP engineId. **(p. 470)**
    - **group** -- Show SNMPv3 User to Group mappings. **(p. 473)**
        - **group < ManagerPriv | ManagerAuth | OperatorAuth | ... >** -- Show SNMPv3 users. **(p. 473)**
            - **user** -- Show a specific user. (ASCII-STR) **(p. 516)**
                - **sec-model < ver1 | ver2c | ver3 >** -- Show a specific security model. **(p. 506)**
    - **notify** -- Show SNMPv3 notification table. **(p. 493)**
        - **NOTIFY-NAME** -- Show a specific notification entry. (ASCII-STR) **(p. 493)**
    - **only** -- Show SNMP message reception policy. **(p. 493)**
    - **params** -- Show SNMPv3 Target Parameters table. **(p. 494)**
        - **PARAM-NAME** -- Show a specific Target Parameter entry. (ASCII-STR) **(p. 494)**
    - **restricted-access** -- Show SNMPv1 and SNMPv2c access properties. **(p. 503)**
    - **targetaddress** -- Show SNMPv3 Target Address table. **(p. 513)**
        - **TARGETADDR-NAME** -- Show a specifc target address entry. (ASCII-STR) **(p. 513)**
    - **user** -- Show SNMPv3 users. **(p. 516)**
        - **USER-NAME** -- Show a specific user. (ASCII-STR) **(p. 516)**
    - **view** -- Show views. **(p. 517)**
        - **VIEW-NAME** -- Set view name. (ASCII-STR) **(p. 517)**
            - **SUB-TREE** -- Set the OID of the tree. (ASCII-STR) **(p. 512)**
- show **sntp** -- Show configured time protocol and servers **(p. 508)**
- show **spanning-tree** -- Show spanning tree information **(p. 509)**
    - **bpdu-protection** -- Show spanning tree BPDU protection status information. **(p. 458)**
        - **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**
    - **config** -- Show spanning tree configuration information. **(p. 462)**
        - **instance** -- Show the spanning tree instance information. **(p. 477)**
            - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 483)**
            - **MSTID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 491)**
    - **debug-counters** -- Show spanning tree debug counters information. **(p. 467)**
        - **instance < 0 to 16 >** -- Show spanning tree instance debug counters information. (NUMBER) **(p. 477)**
            - **ports** -- Show spanning tree port(s) debug counters information. ([ethernet] PORT-LIST) **(p. 498)**

    - **ports** -- Show spanning tree port(s) debug counters information. ([ethernet] PORT-LIST) **(p. 498)**
      - **instance < 0 to 16 >** -- Show spanning tree instance debug counters information. (NUMBER) **(p. 477)**
  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 467)**
  - **instance** -- Show the spanning tree instance information. **(p. 477)**
    - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 483)**
      - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 467)**
    - **MSTID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 491)**
      - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 467)**
  - **mst-config** -- Show multiple spanning tree region configuration. **(p. 491)**
  - **pending** -- Show spanning tree pending configuration **(p. 495)**
    - **instance** -- Show multiple spanning tree instance pending configuration information. **(p. 477)**
      - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 483)**
      - **MSTID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 491)**
    - **mst-config** -- Show multiple spanning tree pending region configuration. **(p. 491)**
  - **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**
    - **config** -- Show spanning tree configuration information. **(p. 462)**
      - **instance** -- Show the spanning tree instance information. **(p. 477)**
        - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 483)**
        - **MSTID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 491)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 467)**
    - **instance** -- Show spanning tree instance status information. **(p. 477)**
      - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 483)**
        - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 467)**
      - **MSTID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 491)**
        - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 467)**
  - **pvst-filter** -- Show spanning tree PVST filter status information. **(p. 499)**
    - **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**
  - **pvst-protection** -- Show spanning tree PVST protection status information. **(p. 499)**
    - **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**
  - **root-history** -- Show spanning tree Root changes history information. **(p. 504)**
    - **cst** -- Show CST Root changes history. **(p. 466)**
    - **ist** -- Show IST Regional Root changes history. **(p. 483)**
    - **msti < 1 to 16 >** -- Show MSTI Regional Root changes history. (NUMBER) **(p. 491)**
  - **traps** -- Show spanning tree trap information. **(p. 515)**
- show **stack** -- Show the stack status of this switch **(p. 509)**
  - **all** -- Show information about all the stacks available on the LAN. **(p. 453)**
  - **candidates** -- Show the list of devices that are stack candidates. **(p. 459)**
  - **view** -- Show the list of devices that are stack members. **(p. 517)**
- show **static-mac** -- Show the locked-down MAC addresses in all vlans **(p. 510)**
- show **svlans** -- Show status information for all VLANs **(p. 512)**
  - **ports** -- Show VLANs that have at least one port from the 'PORT-LIST' as a member. ([ethernet] PORT-LIST) **(p. 498)**
    - **detail** -- Display more info for each port from the 'PORT-LIST' separately. **(p. 467)**
  - **vlan** -- Show detailed VLAN information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**

- show **system** -- Show global configured and operational system paramaters (default is information) **(p. 512)**
  - **fans** -- Show system fan status **(p. 471)**
  - **information** -- Show global configured and operational system parameters **(p. 477)**
  - **power-supply** -- Show Chassis Power Supply info and settings **(p. 499)**
  - **temperature** -- Show systems temperatures and settings **(p. 514)**
- show **tacacs** -- Show TACACS status and statistics **(p. 513)**
- show **tech** -- Display output of a predefined command sequence used by technical support **(p. 513)**
  - **all** -- Display output of a predefined command sequence used by technical support **(p. 453)**
  - **buffers** -- Display output of a predefined command sequence used by technical support **(p. 459)**
  - **instrumentation** -- Display output of a predefined command sequence used by technical support **(p. 478)**
  - **mesh** -- Display output of a predefined command sequence used by technical support **(p. 488)**
  - **route** -- Display output of a predefined command sequence used by technical support **(p. 504)**
  - **statistics** -- Display output of a predefined command sequence used by technical support **(p. 510)**
  - **transceivers** -- Display output of a predefined command sequence used by technical support **(p. 514)**
- show **telnet** -- Show active incoming and outgoing sessions **(p. 514)**
- show **terminal** -- Show logical window dimensions **(p. 514)**
- show **time** -- Show current date and time **(p. 514)**
- show **timep** -- Show configured time protocol and servers **(p. 514)**
- show **trunks** -- Show a list of ports and the trunks to which they belong **(p. 515)**
  - **port-list** -- Show the trunk information only for the ports specified. ([ethernet] PORT-LIST) **(p. 496)**
- show **uptime** -- Displays elapsed time since last boot **(p. 516)**
- show **version** -- Show software version **(p. 517)**
- show **vlans** -- Show status information for all VLANs **(p. 521)**
  - **ports** -- Show VLANs that have at least one port from the 'PORT-LIST' as a member. ([ethernet] PORT-LIST) **(p. 498)**
    - **detail** -- Display more info for each port from the 'PORT-LIST' separately. **(p. 467)**
  - **vlan** -- Show detailed VLAN information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**
- show **vrrp** -- Show VRRP configuration and statistics information **(p. 522)**
  - **config** -- Show VRRP configuration information for the device **(p. 462)**
    - **global** -- Show global VRRP configuration information. **(p. 473)**
  - **statistics** -- Show VRRP statistics information for the device **(p. 510)**
    - **global** -- Show global VRRP configuration information. **(p. 473)**
  - **vlan** -- Show VRRP information for a VLAN. **(p. 518)**
    - **VLAN-ID** -- Specify VLAN for which to display VRRP information. (VLAN-ID) **(p. 520)**
      - **config** -- Show VRRP configuration information for the VLAN. **(p. 462)**
      - **statistics** -- Show VRRP statistics information for the VLAN. **(p. 510)**
      - **vrid** -- Show information for a virtual router. **(p. 521)**
        - **VRID < 1 to 255 >** -- Specify virtual router for which to display information. **(p. 522)**
          - **config** -- Show virtual router configuration information. **(p. 462)**
          - **statistics** -- Show virtual router statistics information. **(p. 510)**
- show **wireless-services** -- Show wireless-services information **(p. 523)**
  - **vlans** -- Display all radio-port VLANs. **(p. 521)**
  - **wireless-services** -- Show wireless-services information (SLOT-ID) **(p. 523)**
    - **radio-ports** -- Display radio-ports associated with a wireless-services module. **(p. 500)**
    - **uplinks** -- Display uplink ports associated with a wireless-services module. **(p. 516)**

COMMAND DETAILS

cst (p. 466)
debug (p. 466)
debug-counters (p. 467)
delayed-flush (p. 467)
destination (p. 467)
detail (p. 467)
detailed (p. 468)
device-priority (p. 469)
dhcp-relay (p. 469)
dhcp-snooping (p. 469)
dns (p. 469)
domains (p. 469)
dscp-map (p. 470)
dyn-authorization (p. 470)
elected (p. 470)
enable (p. 470)
endpoint (p. 470)
engineid (p. 470)
entries (p. 470)
event_class (p. 470)
external-link-state (p. 471)
fans (p. 471)
fastboot (p. 471)
fault-finder (p. 471)
filename (p. 471)
files (p. 471)
filter (p. 472)
fingerprint (p. 472)
flash (p. 472)
forward-protocol (p. 472)
front-panel-security (p. 473)
general (p. 473)
global (p. 473)
group (p. 473)
gvrp (p. 474)
hc (p. 474)
mroute (p. 490)
mst-config (p. 491)
msti (p. 491)
MSTID (p. 491)
name (p. 492)
neighbor (p. 492)
neighbor-ip (p. 492)
neighbors (p. 492)
neighbors-port (p. 493)
notify (p. 493)
NOTIFY-NAME (p. 493)
only (p. 493)
option (p. 493)
ospf (p. 493)
output (p. 494)
PARAM-NAME (p. 494)
params (p. 494)
peer (p. 494)
peer-ip (p. 494)
pending (p. 495)
pim (p. 495)
port-access (p. 495)
port-list (p. 496)
port-priority (p. 497)
ports (p. 498)
port-security (p. 498)
port-utilization (p. 498)
power-over-ethernet (p. 499)
power-supply (p. 499)
protocol-priority (p. 499)
pvst-filter (p. 499)
pvst-protection (p. 499)
qinq (p. 500)
qos (p. 500)
queue-config (p. 500)
-r (p. 500)
terminal (p. 514)
throttled-hosts (p. 514)
time (p. 514)
timep (p. 514)
transceivers (p. 514)
traps (p. 515)
trunks (p. 515)
type (p. 515)
type-of-service (p. 516)
uninstalled (p. 516)
uplinks (p. 516)
uptime (p. 516)
user (p. 516)
USER-NAME (p. 516)
ver1-2c (p. 516)
ver3 (p. 517)
version (p. 517)
view (p. 517)
VIEW-NAME (p. 517)
virtual-link (p. 517)
virtual-neighbor (p. 518)
vlan (p. 518)
vlan-id (p. 520)
VLAN-ID (p. 520)
vlan-priority (p. 521)
vlans (p. 521)
vlink-ip (p. 521)
vneighbor-ip (p. 521)
vrid (p. 521)
VRID (p. 522)
vrrp (p. 522)
web-based (p. 522)
web-server (p. 523)
wireless-services (p. 523)

- show port-access authenticator *[ETHERNET] PORT-LIST*

```
Show information for specified ports only.
```

Next Available Options:

- **config** -- Show 802.1X authenticator configuration.**(p. 462)**
- **statistics** -- Show authentication sessions statistics for 802.1X authenticator.**(p. 510)**
- **session-counters** -- Show 802.1X current (or last if no current sessions open) sessions counters.**(p. 506)**
- **vlan** -- Show authorized and unauthorized vlans for 802.1X authenticator.**(p. 518)**
- **clients** -- Show the current 802.1X client session statistics. **(p. 460)**

- show port-access authenticator clients *[ETHERNET] PORT-LIST*

```
Show information for specified ports only.
```

Next Available Option:

- **detailed** -- Show the current 802.1X client session detailed statistics. **(p. 468)**

- show port-access supplicant *[ETHERNET] PORT-LIST*

  `Show information for specified ports only.`

- show port-access mac-based *[ETHERNET] PORT-LIST*

  `Specify ports for which MAC Authentication information will be shown.`

Next Available Options:

- **config** -- Show the current configuration of MAC Authentication.**(p. 462)**
- **clients** -- Show the connected MAC address information.**(p. 460)**

- show port-access mac-based config *[ETHERNET] PORT-LIST*

  `Specify ports for which MAC Authentication information will be shown.`

Next Available Options:

- **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
- **detailed** -- Show the detailed configuration of MAC Authentication.**(p. 468)**

- show port-access mac-based clients *[ETHERNET] PORT-LIST*

  `Specify ports for which MAC Authentication information will be shown.`

Next Available Option:

- **detailed** -- Show the connected MAC address detailed information.**(p. 468)**

- show port-access web-based *[ETHERNET] PORT-LIST*

  `Specify ports for which Web Authentication information will be shown.`

Next Available Options:

- **config** -- Show the current configuration of Web Authentication.**(p. 462)**
- **clients** -- Show the current web client session statistics.**(p. 460)**

- show port-access web-based config *[ETHERNET] PORT-LIST*

  `Specify ports for which Web Authentication information will be shown.`

Next Available Options:

- **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
- **web-server** -- Show the web server-related configuration items.**(p. 523)**
- **detailed** -- Show the detailed configuration of Web Authentication.**(p. 468)**

- show port-access web-based clients *[ETHERNET] PORT-LIST*

  `Specify ports for which Web Authentication information will be shown.`

Next Available Option:

- **detailed** -- Show the current web client session detailed statistics.**(p. 468)**

- show port-access *[ETHERNET] PORT-LIST*

```
Usage: show port-access [PORT-LIST] <mac-based|web-based>...
       show port-access <mac-based|web-based> [PORT-LIST]...

Description: Show Web/MAC Authentication statistics and configuration. If
             PORT-LIST parameter is specified then information only for the
             specified ports is shown.
```

Next Available Options:

- **authenticator** -- Show 802.1X authenticator statistics and configuration. **(p. 455)**
- **mac-based** -- Show MAC Authentication statistics and configuration**(p. 487)**
- **web-based** -- Show Web Authentication statistics and configuration**(p. 522)**

-a

- show logging -a

```
Display all log events, including those from previous boot cycles.
```

access-group

- show rate-limit ip access-group

```
access-group
```

Next Available Option:

- **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**

access-list

- show access-list

```
Usage: show access-list [config] |
                        [vlan <VLAN-ID>] |
                        [<ACL-ID> [config]]

Description: Show Access Control List information.  If no parameters
             are specified, a summary table is displayed.

Parameters:

    o config - Display all configured ACL's on the switch using
               the CLI syntax used to create them.
    o vlan <VLAN-ID> - Display Access Control Lists currently applied
                       to the specified VLAN.
    o <ACL-ID> - Display detailed information on the specified ACL.
    o resources  - Display ACL Rules/Masks availability.
```

Next Available Options:

- **radius** -- Display ACLs applied via RADIUS. ([ethernet] PORT-LIST) **(p. 500)**

- **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 462)**
- **vlan** -- Show ACLs applied to the specified VLAN. (VLAN-ID) **(p. 518)**
- **ports** -- Show ACLs applied to the specified ports. ([ethernet] PORT-LIST) **(p. 498)**
- **acl-name** -- Display detailed information on specified ACL. (ASCII-STR) **(p. 452)**
- **resources** -- Display ACL Rules/Masks availability.**(p. 502)**

access-rights

- show snmpv3 access-rights

```
Show information about access rights.
```

Next Available Option:

- **group** < ManagerPriv | ManagerAuth | OperatorAuth | ... > -- Show SNMPv3 users. **(p. 473)**

accounting

- show accounting

```
Usage: show accounting [sessions]

Description: Show Accounting configuration parameters.
             If 'sessions' is specified then show accounting
             data for all active sessions.
```

Next Available Option:

- **sessions** -- Show accounting data for all active sessions**(p. 507)**

- show radius accounting

```
Usage: show radius accounting

Description: Show RADIUS accounting statistics.
```

acl-name

- show access-list *ACL-NAME*

```
Display detailed information on specified ACL.
```

Next Available Option:

- **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 462)**

address-table-port

- show mac-address *[ETHERNET] PORT-LIST*

```
Show MAC addresses learned on the specified ports.
```

advertise

- show ip ospf external-link-state advertise

```
Show each LSA as a stream of bytes in hexadecimal notation.
```

- show ip ospf link-state advertise

```
Show each LSA as a stream of bytes in hexadecimal notation.
```

agent

- show sflow agent

```
Displays read-only switch agent information: The agent address is normally the ip
address of the first vlan configured.
```

all

- show rate-limit all

```
Show limits for all traffic.
```

Next Available Option:

- **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**

- show stack all

```
Show information about all the stacks available on the LAN.
```

- show tech all

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

all-hosts

- show connection-rate-filter all-hosts

```
Show blocked and throttled IP addresses.
```

area

- show ip ospf area

```
Usage: show ip ospf area [OSPF-AREA-ID]

Description: Show OSPF areas configured on the device. Invoked without
             parameters displays all OSPF areas configured. If the
             'OSPF-AREA-ID' is specified detailed information for
             the correspondent OSPF area is shown.
```

Next Available Option:

- **area-ip** -- (OSPF-AREA-ID) **(p. 454)**

- show ip ospf virtual-neighbor area *OSPF-AREA-ID*

```
Specify area of the virtual neighbors to show.
```

- show ip ospf virtual-link area *OSPF-AREA-ID*

```
Specify area of the virtual links to show.
```

area-id

- show ip ospf link-state *OSPF-AREA-ID*

```
Show LSAs for the specified area only.
```

area-ip

- show ip ospf area *OSPF-AREA-ID*

arp

- show arp

```
Usage: show arp [vlan VLAN-ID]

Description: Show the IP ARP translation table.
             If VLAN-ID is specified, the output is filtered on
             the VLAN-ID.
```

Next Available Option:

- **vlan** -- Specify VLAN for which to show ARP entries. (VLAN-ID) **(p. 518)**

arp-protect

- show arp-protect

```
Usage: show arp-protect [stats <VLAN-ID-RANGE>]

Description: Display Dynamic ARP Protection information.

Parameters:
            o stats - Display ARP Protection VLAN counters.
```

Next Available Option:

- **statistics** -- (VLAN-ID-RANGE) **(p. 510)**

authentication

- show authentication

```
Usage: show authentication

Description: Show Authentication configuration parameters.
```

- show radius authentication

```
Usage: show radius authentication

Description: Show RADIUS authentication statistics.
```

authenticator

- show port-access authenticator

  ```
  Usage: show port-access authenticator [config|statistics|session-counters]

  Description: Show 802.1X (Port Based Network Access) authenticator
               current status, configuration or last session counters.
  ```

  Next Available Options:
  - -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 449)**
  - **config** -- Show 802.1X authenticator configuration.**(p. 462)**
  - **statistics** -- Show authentication sessions statistics for 802.1X authenticator.**(p. 510)**
  - **session-counters** -- Show 802.1X current (or last if no current sessions open) sessions counters.**(p. 506)**
  - **vlan** -- Show authorized and unauthorized vlans for 802.1X authenticator.**(p. 518)**
  - **clients** -- Show the current 802.1X client session statistics. **(p. 460)**

- show port-access *[ETHERNET] PORT-LIST* authenticator

  ```
  Usage: show port-access authenticator [config|statistics|session-counters]

  Description: Show 802.1X (Port Based Network Access) authenticator
               current status, configuration or last session counters.
  ```

  Next Available Options:
  - **config** -- Show 802.1X authenticator configuration.**(p. 462)**
  - **statistics** -- Show authentication sessions statistics for 802.1X authenticator.**(p. 510)**
  - **session-counters** -- Show 802.1X current (or last if no current sessions open) sessions counters.**(p. 506)**
  - **vlan** -- Show authorized and unauthorized vlans for 802.1X authenticator.**(p. 518)**
  - **clients** -- Show the current 802.1X client session statistics. **(p. 460)**

authorization

- show authorization

  ```
  Usage: show authorization

  Description: Show Authorization configuration parameters.
  ```

authorized-managers

- show ip authorized-managers

  ```
  Usage: show ip authorized-managers

  Description: Show IPV4 addresses allowed to manage the switch.
  ```

- show ipv6 authorized-managers

  ```
  Usage: show ipv6 authorized-managers

  Description: Show IPV6 addresses allowed to manage the switch.
  ```

auth-server

- show port-access mac-based *[ETHERNET] PORT-LIST* config auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access mac-based config *[ETHERNET] PORT-LIST* auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access mac-based config auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access web-based *[ETHERNET] PORT-LIST* config auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access web-based config *[ETHERNET] PORT-LIST* auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access web-based config auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access *[ETHERNET] PORT-LIST* mac-based config auth-server

  ```
  Show the authentication server-related configuration items.
  ```

- show port-access *[ETHERNET] PORT-LIST* web-based config auth-server

  ```
  Show the authentication server-related configuration items.
  ```

auto-provision

- show lldp auto-provision

  ```
  Usage: show lldp auto-provision radio-ports

  Description: Show LLDP auto-provision related info for radio-ports.
  ```

  Next Available Option:

  - **radio-ports** -- Show LLDP radio-ports information.**(p. 500)**

autorun

- show autorun

  ```
  Show Autorun configuration status.
  ```

autorun-cert

- show crypto autorun-cert

  ```
  Display trusted certificate.
  ```

autorun-key

- show crypto autorun-key

```
Display autorun key.
```

babble

- show crypto client-public-key babble

```
Display phonetic hash.
```

- show crypto client-public-key *< manager | operator >* babble

```
Display phonetic hash.
```

- show crypto client-public-key *< manager | operator > KEYLIST* babble

```
Display phonetic hash.
```

- show crypto host-public-key babble

```
Display phonetic hash.
```

- show ip client-public-key babble

```
Display phonetic hash.
```

- show ip host-public-key babble

```
Display phonetic hash.
```

bandwidth

- show bandwidth

```
Usage: show bandwidth <output> [PORT-LIST]

Description: Show queue percentages for outbound guaranteed minimum
             bandwidth. If PORT-LIST parameter is specified, information
             is shown only for the specified ports.
```

Next Available Option:

- **output** -- Show outbound guaranteed minimum bandwidth.**(p. 494)**

banner

- show banner

```
Usage: show banner motd

Description: show the configured banner text.
```

Next Available Option:

- **motd** -- show the configured banner text**(p. 490)**

binding

- show dhcp-snooping binding

```
Display DHCP snooping binding information.
```

blocked-hosts

- show connection-rate-filter blocked-hosts

```
Show blocked IP addresses.
```

boot-history

- show boot-history

```
Usage: show boot-history

Description: Display the system boot log.
```

bpdu-protection

- show spanning-tree bpdu-protection

```
Show spanning tree BPDU protection status information.
```

Next Available Option:

- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**

brief

- show interfaces brief

```
Usage: show interfaces brief

Description: Show the ports' operational parameters.
```

Next Available Option:

- **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 496)**

- show power-over-ethernet brief

```
Usage: show power-over-ethernet brief

Description: Show summary of poe status.
```

Next Available Options:

- **port-list** -- Show the ports' poe status ([ethernet] PORT-LIST) **(p. 496)**
- **slot** -- Show summary of poe status (SLOT-ID-RANGE) **(p. 507)**

bsr

- show ip pim bsr

```
Usage: show ip pim bsr [elected|local]

Description: Show Bootstrap Router information. When invoked without parameters
             displays the information about currently elected BSR and the local
             Candidate-BSR and Candidate-RP information.
```

Next Available Options:

- **elected** -- Show elected Bootstrap Router information. **(p. 470)**
- **local** -- Show local Candidate-BSR configuration information. **(p. 486)**

buffer

- show debug buffer

```
Show the contents of the debug log buffer.
```

buffers

- show tech buffers

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

candidates

- show stack candidates

```
Show the list of devices that are stack candidates.
```

cdp

- show cdp

```
Usage: show cdp [neighbor [PORT-NUM] [detail]]

Description: Show CDP configuration and neighbors discovered.
             Legend for 'capability' field of the 'show cdp neighbor'
             command output:
             R - Performs level 3 routing for at least one network
                 layer protocol.
             B - Performs level 2 transparent bridging.
             Bs - Performs level 2 source-route bridging.
             S - Performs level 2 switching.
             P - Sends and receives packets for at least one network
                 layer protocol.
             In - The bridge or switch does not forward IGMP Report packets.
             L1 - Provides level 1 functionality.
```

Next Available Option:

- **neighbors** -- Show CDP neighbors. See 'show cdp help' for details.**(p. 492)**

CHAIN-NAME

- show key-chain *CHAIN-NAME*

```
Show the chain detailed information.
```

client-public-key

- show crypto client-public-key

```
Display ssh authorized client public keys.
```

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 457)**
- **fingerprint** -- Display hexadecimal hash.**(p. 472)**
- **keyfile** < manager | operator > -- Choose to display manager or operator keys.**(p. 484)**

- show ip client-public-key

```
Usage: show ip client-public-key [babble|fingerprint]

Description: Show currently loaded public keys for authorized clients.
             The 'babble' and 'fingerprint' options produce a phonetic or
             hexadecimal hash instead of displaying the raw key file.
```

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 457)**
- **fingerprint** -- Display hexadecimal hash.**(p. 472)**

clients

- show port-access authenticator *[ETHERNET] PORT-LIST* clients

```
Show the current 802.1X client session statistics.
```

Next Available Option:

- **detailed** -- Show the current 802.1X client session detailed statistics. **(p. 468)**

- show port-access authenticator clients

```
Show the current 802.1X client session statistics.
```

Next Available Option:

- -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 449)**

- show port-access mac-based *[ETHERNET] PORT-LIST* clients

```
Show the connected MAC address information.
```

Next Available Option:

- **detailed** -- Show the connected MAC address detailed information.**(p. 468)**

- show port-access mac-based clients

```
Show the connected MAC address information.
```

Next Available Option:

- -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**

- show port-access web-based *[ETHERNET] PORT-LIST* clients

```
Show the current web client session statistics.
```

Next Available Option:

- **detailed** -- Show the current web client session detailed statistics.**(p. 468)**

- show port-access web-based clients

  ```
  Show the current web client session statistics.
  ```

  Next Available Option:

  - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**

- show port-access *[ETHERNET] PORT-LIST* authenticator clients

  ```
  Show the current 802.1X client session statistics.
  ```

  Next Available Option:

  - **detailed** -- Show the current 802.1X client session detailed statistics. **(p. 468)**

- show port-access *[ETHERNET] PORT-LIST* mac-based clients

  ```
  Show the connected MAC address information.
  ```

  Next Available Option:

  - **detailed** -- Show the connected MAC address detailed information.**(p. 468)**

- show port-access *[ETHERNET] PORT-LIST* web-based clients

  ```
  Show the current web client session statistics.
  ```

  Next Available Option:

  - **detailed** -- Show the current web client session detailed statistics.**(p. 468)**

community

- show snmp-server *COMMUNITY*

  ```
  Specify SNMP community to which to restrict the output.
  ```

- show snmpv3 community

  ```
  Show SNMPv3 Community table.
  ```

  Next Available Option:

  - **COMMUNITY-NAME** -- Show a specific community entry. (ASCII-STR) **(p. 461)**

COMMUNITY-NAME

- show snmpv3 community *COMMUNITY-NAME*

  ```
  Show a specific community entry.
  ```

config

- show access-list config

```
Show all configured ACL's on the switch using
                            the CLI syntax used to create them.
```

- show access-list *ACL-NAME* config

```
Show all configured ACL's on the switch using
                            the CLI syntax used to create them.
```

- show config

```
Usage: show config [files | FILENAME | status]

Description: Show the switch startup configuration.

Parameters:

    o files - list switch configuration files.  Shows which file is active
              and which are associated with primary and secondary images.
    o FILENAME - show specified configuration instead of active configuration.
    o status - check if there are changes in running configuration not
              saved to the startup configuration file.
```

Next Available Options:

- **status** -- Check if the running configuration differs from the statup configuration.**(p. 511)**
- **files** -- List saved configuration files.**(p. 471)**
- **filename** < config | new > -- Display specified configuration.**(p. 471)**

- show interfaces config

```
Usage: show interfaces config

Description: Show configuration information.
```

- show ip igmp *VLAN-ID* config

```
Show IGMP configuration information for the VLAN specified.
```

- show ip igmp config

```
Show IGMP configuration information.
```

- show ip pim rp-candidate config

```
Show C-RP configuration information.
```

- show ipv6 mld vlan *VLAN-ID* config

```
Show MLD configuration information for the VLAN specified.
```

- show ipv6 mld config

```
Show MLD configuration information.
```

- show lldp config

```
Usage: show lldp config [[ethernet] PORT-LIST]]
```

```
Description: Show LLDP configuration information.
    o [ethernet] PORT-LIST - Show port configuration information.
```

Next Available Option:

- **port-list** -- Specify the port or list of ports. ([ethernet] PORT-LIST) **(p. 496)**

- show port-access authenticator *[ETHERNET] PORT-LIST* config

```
Show 802.1X authenticator configuration.
```

- show port-access authenticator config

```
Show 802.1X authenticator configuration.
```

- show port-access mac-based *[ETHERNET] PORT-LIST* config

```
Show the current configuration of MAC Authentication.
```

Next Available Options:

- **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
- **detailed** -- Show the detailed configuration of MAC Authentication.**(p. 468)**

- show port-access mac-based config

```
Show the current configuration of MAC Authentication.
```

Next Available Options:

- -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
- **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**

- show port-access web-based *[ETHERNET] PORT-LIST* config

```
Show the current configuration of Web Authentication.
```

Next Available Options:

- **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
- **web-server** -- Show the web server-related configuration items.**(p. 523)**
- **detailed** -- Show the detailed configuration of Web Authentication.**(p. 468)**

- show port-access web-based config

```
Show the current configuration of Web Authentication.
```

Next Available Options:

- -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
- **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
- **web-server** -- Show the web server-related configuration items.**(p. 523)**

- show port-access *[ETHERNET] PORT-LIST* authenticator config

```
Show 802.1X authenticator configuration.
```

- show port-access *[ETHERNET] PORT-LIST* mac-based config

  ```
  Show the current configuration of MAC Authentication.
  ```

  Next Available Options:
  - **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
  - **detailed** -- Show the detailed configuration of MAC Authentication.**(p. 468)**

- show port-access *[ETHERNET] PORT-LIST* web-based config

  ```
  Show the current configuration of Web Authentication.
  ```

  Next Available Options:
  - **auth-server** -- Show the authentication server-related configuration items.**(p. 456)**
  - **web-server** -- Show the web server-related configuration items.**(p. 523)**
  - **detailed** -- Show the detailed configuration of Web Authentication.**(p. 468)**

- show port-access config

  ```
  Show status of 802.1X, Web Auth, and MAC Auth configurations.
  ```

- show spanning-tree *[ETHERNET] PORT-LIST* config

  ```
  Show spanning tree configuration information.
  ```

  Next Available Option:
  - **instance** -- Show the spanning tree instance information.**(p. 477)**

- show spanning-tree config

  ```
  Show spanning tree configuration information.
  ```

  Next Available Option:
  - **instance** -- Show the spanning tree instance information.**(p. 477)**

- show vrrp config

  ```
  Usage: show vrrp config

  Description: Show VRRP configuration information for the device.
  ```

  Next Available Option:
  - **global** -- Show global VRRP configuration information. **(p. 473)**

- show vrrp vlan *VLAN-ID* config

  ```
  Show VRRP configuration information for the VLAN.
  ```

- show vrrp vlan *VLAN-ID* vrid *< 1 to 255 >* config

  ```
  Show virtual router configuration information.
  ```

configuration

- show instrumentation monitor configuration

```
Usage: show instrumentation monitor configuration

Description: show configured thresholds for monitored parameters.
             shows the parameter name and the configured threshold
             value for all parameters.
             If instrumenation monitoring for the particular paramter
             is disabled then threshold for the particular parameter is
             displayed as 'Not Monitored'.
```

connection-rate-filter

- show connection-rate-filter

```
Usage: show connection-rate-filter [all-hosts] [blocked-hosts] [throttled-hosts]

Description: List the ports and the on/off connection-rate-filter status and
             sensitivity.

Parameters:
    o all-hosts       - Display the IP addresses of the hosts that are blocked
                        and throttled
    o blocked-hosts   - Print the IP addresses of the hosts that are currently
                        blocked
    o throttled-hosts - Print the IP addresses of the hosts that are currently
                        throttled
```

Next Available Options:

- **all-hosts** -- Show blocked and throttled IP addresses.**(p. 453)**
- **blocked-hosts** -- Show blocked IP addresses.**(p. 458)**
- **throttled-hosts** -- Show throttled IP addresses.**(p. 514)**

console

- show console

```
Usage: show console

Description: Show serial link/console settings.
```

counters

- show ipv6 mld vlan *VLAN-ID* counters

```
Show MLD VLAN counter information.
```

cpu

- show cpu

```
Usage: show cpu [<1-300>]
                [slot <SLOT-LIST> [<1-90>] ]

Description: Show average CPU utilization over the last 1, 5, and 60 seconds;
             or the number of seconds specified.
```

```
Use the 'slot' argument to display CPU utilization for the
specified modules, rather than the chassis CPU.
```

Next Available Options:

- **time** < 1 to 300 > -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 514)**
- **slot** -- Display module CPU statistics. (SLOT-ID-RANGE) **(p. 507)**

crypto

- show crypto

```
Usage: show crypto client-public-key [INDEX] [<fingerprint|babble>]
                   host-public-key [<fingerprint|babble>]
                   host-cert
                   autorun-key

Description: Display flash files used for authentication.

Parameters:

    o client-public-key - display keys used by ssh for client public
             key authentication.
    o INDEX - specify a single client public key, with more detailed
             output.
    o <fingerprint|babble> - display a hexadecimal or phonetic hash
             of the key[s].
    o host-public-key - display the ssh host public key.
    o host-cert - display the device's ssl host certificate.
    o autorun-key - display autorun key.
    o autorun-cert - display trusted certificate.
```

Next Available Options:

- **client-public-key** -- Display ssh authorized client public keys.**(p. 459)**
- **host-public-key** -- Display ssh host RSA public key.**(p. 475)**
- **host-cert** -- Display https certificate information.**(p. 475)**
- **autorun-key** -- Display autorun key.**(p. 456)**
- **autorun-cert** -- Display trusted certificate.**(p. 456)**

cst

- show spanning-tree root-history cst

```
Show CST Root changes history.
```

debug

- show debug

```
Usage: show debug

Description: Display currently active debug log destinations and types.

Parameters:
    o buffer - Show the contents of the in-memory debug buffer
```

Next Available Option:

- **buffer** -- Show the contents of the debug log buffer.**(p. 459)**

debug-counters

- show spanning-tree debug-counters

```
Show spanning tree debug counters information.
```

Next Available Options:

- **instance** < 0 to 16 > -- Show spanning tree instance debug counters information. (NUMBER) **(p. 477)**
- **ports** -- Show spanning tree port(s) debug counters information. ([ethernet] PORT-LIST) **(p. 498)**

delayed-flush

- show igmp delayed-flush

```
Usage: show igmp delayed-flush

Description: Shows switch-wide IGMP delayed flush value.
```

destination

- show sflow *< 1 to 3 >* destination

```
Displays information about the receiver/collector/management-station to which the
sampling-polling data is sent.
```

detail

- show cdp neighbors detail

```
Show neighbor information field-per-line instead of shortened table format.
```

- show spanning-tree *[ETHERNET] PORT-LIST* detail

```
Show spanning tree extended details Port, Bridge, Rx, and Tx report.
```

- show spanning-tree *[ETHERNET] PORT-LIST* instance ist detail

```
Show spanning tree extended details Port, Bridge, Rx, and Tx report.
```

- show spanning-tree *[ETHERNET] PORT-LIST* instance *< 1 to 16 >* detail

```
Show spanning tree extended details Port, Bridge, Rx, and Tx report.
```

- show spanning-tree detail

```
Show spanning tree extended details Port, Bridge, Rx, and Tx report.
```

- show spanning-tree instance ist detail

```
Show spanning tree extended details Port, Bridge, Rx, and Tx report.
```

- show spanning-tree instance *< 1 to 16 >* detail

```
Show spanning tree extended details Port, Bridge, Rx, and Tx report.
```

- show vlans ports *[ETHERNET] PORT-LIST* detail

```
Display more info for each port from the 'PORT-LIST' separately.
```

- show svlans ports *[ETHERNET] PORT-LIST* detail

```
Display more info for each port from the 'PORT-LIST' separately.
```

detailed

- show port-access authenticator *[ETHERNET] PORT-LIST* clients detailed

```
Show the current 802.1X client session detailed statistics.
```

- show port-access authenticator clients *[ETHERNET] PORT-LIST* detailed

```
Show the current 802.1X client session detailed statistics.
```

- show port-access mac-based *[ETHERNET] PORT-LIST* config detailed

```
Show the detailed configuration of MAC Authentication.
```

- show port-access mac-based *[ETHERNET] PORT-LIST* clients detailed

```
Show the connected MAC address detailed information.
```

- show port-access mac-based config *[ETHERNET] PORT-LIST* detailed

```
Show the detailed configuration of MAC Authentication.
```

- show port-access mac-based clients *[ETHERNET] PORT-LIST* detailed

```
Show the connected MAC address detailed information.
```

- show port-access web-based *[ETHERNET] PORT-LIST* config detailed

```
Show the detailed configuration of Web Authentication.
```

- show port-access web-based *[ETHERNET] PORT-LIST* clients detailed

```
Show the current web client session detailed statistics.
```

- show port-access web-based config *[ETHERNET] PORT-LIST* detailed

```
Show the detailed configuration of Web Authentication.
```

- show port-access web-based clients *[ETHERNET] PORT-LIST* detailed

```
Show the current web client session detailed statistics.
```

- show port-access *[ETHERNET] PORT-LIST* authenticator clients detailed

```
Show the current 802.1X client session detailed statistics.
```

- show port-access *[ETHERNET] PORT-LIST* mac-based config detailed

```
Show the detailed configuration of MAC Authentication.
```

- show port-access *[ETHERNET] PORT-LIST* mac-based clients detailed

```
Show the connected MAC address detailed information.
```

- show port-access *[ETHERNET] PORT-LIST* web-based config detailed

```
Show the detailed configuration of Web Authentication.
```

- show port-access *[ETHERNET] PORT-LIST* web-based clients detailed

```
Show the current web client session detailed statistics.
```

device-priority

- show qos device-priority

```
Usage: show qos device-priority

Description: Show the device priority table (priority based on
             the IP addresses).
```

dhcp-relay

- show dhcp-relay

```
Usage: show dhcp-relay

Description: Shows the current status of DHCP Relay Agent and
             option 82 statistics.
```

dhcp-snooping

- show dhcp-snooping

```
Usage: show dhcp-snooping [<binding|stats>]

Description: Display DHCP snooping information.

Parameters:

            o binding - Display DHCP snooping binding information.

            o stats   - Display DHCP snooping events.
```

Next Available Options:

- **binding** -- Display DHCP snooping binding information.**(p. 457)**
- **stats** -- Display DHCP snooping events.**(p. 511)**

dns

- show ip dns

```
Usage: show ip dns

Description: Show configured DNS server IP addresses on the switch.
```

domains

- show igmp-proxy domains

```
Show all the currently configured IGMP proxy domains.
```

dscp-map

- show qos dscp-map

```
Usage: qos dscp-map

Description: Show mappings between DSCP policy and 802.1p priority.
```

dyn-authorization

- show radius dyn-authorization

```
Usage: show radius dynamic authorization

Description: Show RADIUS dynamic authorization statistics.
```

- show radius host *IP-ADDR* dyn-authorization

elected

- show ip pim bsr elected

```
Show elected Bootstrap Router information.
```

enable

- show snmpv3 enable

```
Show SNMPv3 status.
```

endpoint

- show monitor endpoint

```
Remote mirroring destination configuration.
```

engineid

- show snmpv3 engineid

```
Show switch's SNMP engineId.
```

entries

- show igmp-proxy entries

```
Show all the currently active IGMP proxy entries.
```

event_class

- show logging

```
Specify substring to match in log entry. See 'log help' for details.
```

Supported Values:

- **-M** -- Major event class.
- **-P** -- Performance event class.
- **-W** -- Warning event class.
- **-I** -- Information event class.
- **-D** -- Debug event class.

external-link-state

- show ip ospf external-link-state

  ```
  Usage: show ip ospf external-link-state [status|advertise]

  Description: Show the Link State Advertisements from throughout
               the areas to which the device is attached. The command
               shows only External Link State Advertisements.
               The 'status' keyword is optional and does not affect the
               command output. If the 'advertise' is specified, each LSA
               is shown as a stream of bytes in hexadecimal notation.
  ```

  Next Available Options:

  - **status** -- The keyword is optional and can be omitted.**(p. 511)**
  - **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation.**(p. 452)**
  - **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 485)**
  - **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 505)**
  - **sequence-number** -- Show LSAs with the specified sequence number only.**(p. 506)**

fans

- show system fans

  ```
  Usage: show system fans

  Description: Show system fan status.
  ```

fastboot

- show fastboot

  ```
  Usage: show fastboot

  Description: Shows the current status of fastboot on switch.
  ```

fault-finder

- show fault-finder

  ```
  Usage: show fault-finder

  Description: Show the fault-finder table.
  ```

filename

- show config *< config | new >*

  ```
  Display specified configuration.
  ```

  Supported Values:

  - **config**
  - **new**

files

- show config files

  ```
  List saved configuration files.
  ```

filter

- show filter

```
Usage: show filter [INDEX]

Description: Show a table of security filters or a filter
             detailed information, if the filter's INDEX is specified.
```

Next Available Options:

- **INDEX** -- Show detailed information for the filter identified by the INDEX. The indices are displayed by the 'show filter' command.**(p. 477)**
- **source-port** -- **(p. 508)**

fingerprint

- show crypto client-public-key fingerprint

```
Display hexadecimal hash.
```

- show crypto client-public-key < *manager* | *operator* > fingerprint

```
Display hexadecimal hash.
```

- show crypto client-public-key < *manager* | *operator* > *KEYLIST* fingerprint

```
Display hexadecimal hash.
```

- show crypto host-public-key fingerprint

```
Display hexadecimal hash.
```

- show ip client-public-key fingerprint

```
Display hexadecimal hash.
```

- show ip host-public-key fingerprint

```
Display hexadecimal hash.
```

flash

- show flash

```
Usage: show flash

Description: Show the version of software stored in the Primary
             and Secondary image locations.
```

forward-protocol

- show ip forward-protocol

```
Usage: show ip forward-protocol [vlan <VLAN-ID>]

Description: Show server addresses where broadcast requests received by the
             switch are to be forwarded based on configured port.
```

Next Available Option:

- **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 518)**

front-panel-security

- show front-panel-security

```
Usage: show front-panel-security

Description: Show current security status of the front panel butons.  If
             'password-clear' is disabled, the password(s) cannot be reset using
             the clear button on the front panel of the device.  If 'factory-
             reset' is disabled, the configuation/password(s) can not be reset
             using the clear and reset button combination at boot time.  With
             'password-recovery' enabled (and the front panel buttons disabled),
             a lost password can be recovered by contacting HP customer support.
             With 'password-recovery' disabled, there is no way to access a
             device after losing a password with the front panel buttons
             disabled.
```

general

- show ip ospf general

```
Usage: show ip ospf general

Description: Show OSPF basic configuration and operational information.
```

- show ip rip general

```
Usage: show ip rip general

Description: Show RIP basic configuration and operational information.
```

global

- show vrrp config global

```
Show global VRRP configuration information.
```

- show vrrp statistics global

```
Show global VRRP configuration information.
```

group

- show ip igmp group *IP-ADDR*

```
Show ports the specified multicast group address is registered on.
```

- show ipv6 mld vlan *VLAN-ID* group

```
Show MLD VLAN group info.
```

Next Available Option:

- **ipv6-addr** -- Show MLD VLAN group address information. (IPV6-ADDR) **(p. 482)**

- show snmpv3 access-rights *< ManagerPriv | ManagerAuth | OperatorAuth | ... >*

```
Show SNMPv3 users.
```

Supported Values:

- **ManagerPriv** -- Require privacy and authentication, can access all objects.
- **ManagerAuth** -- Require authentication, can access all objects.
- **OperatorAuth** -- Requires authentication, limited access to objects.
- **OperatorNoAuth** -- No authentication required, limited access to objects.
- **ComManagerRW** -- Community with manager and unrestricted write access.
- **ComManagerR** -- Community with manager and restricted write access.
- **ComOperatorRW** -- Community with operator and unrestricted write access.
- **ComOperatorR** -- Community with operator and restricted write access.

Next Available Option:

- **sec-model** -- Set security model. **(p. 506)**

- show snmpv3 group

```
Show SNMPv3 User to Group mappings.
```

Next Available Option:

- **group** < ManagerPriv | ManagerAuth | OperatorAuth | ... > -- Show SNMPv3 users. **(p. 473)**

- show snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >*

```
Show SNMPv3 users.
```

Supported Values:

- **ManagerPriv** -- Require privacy and authentication, can access all objects.
- **ManagerAuth** -- Require authentication, can access all objects.
- **OperatorAuth** -- Requires authentication, limited access to objects.
- **OperatorNoAuth** -- No authentication required, limited access to objects.
- **ComManagerRW** -- Community with manager and unrestricted write access.
- **ComManagerR** -- Community with manager and restricted write access.
- **ComOperatorRW** -- Community with operator and unrestricted write access.
- **ComOperatorR** -- Community with operator and restricted write access.

Next Available Option:

- **user** -- Show a specific user. (ASCII-STR) **(p. 516)**

gvrp

- show gvrp

```
Usage: show gvrp

Description: Show GVRP settings.
```

hc

- show interfaces *[ETHERNET] PORT-LIST* hc

```
Usage: show interfaces [ethernet] PORT-LIST

Description: Show summary of network traffic handled by the ports.
```

helper-address

- show ip helper-address

```
Usage: show ip helper-address [vlan <VLAN-ID>]

Description: Show DHCP servers where DHCP requests received by the
             switch are to be forwarded.
```

Next Available Option:

- **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 518)**

history

- show history

```
Usage: show history

Description: Show previously entered commands.
```

host

- show radius host *IP-ADDR*

```
Usage: show radius host <IP-ADDR>

Description: Show statistics information for the RADIUS host.
```

Next Available Option:

- **dyn-authorization** -- **(p. 470)**

host-cert

- show crypto host-cert

```
Display https certificate information.
```

host-public-key

- show crypto host-public-key

```
Display ssh host RSA public key.
```

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 457)**
- **fingerprint** -- Display hexadecimal hash.**(p. 472)**

- show ip host-public-key

```
Usage: show ip host-public-key [babble|fingerprint]

Description: Display the SSH host RSA public key.  The 'babble' and
             'fingerprint' options display a phonetic or hexadecimal
             hash instead of displaying the numeric values.
```

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 457)**

- **fingerprint** -- Display hexadecimal hash.**(p. 472)**

icmp

- show ip icmp

  ```
  Usage: show ip icmp

  Description: Show ICMP Rate Limiting settings.
  ```

- show rate-limit icmp

  ```
  Show only limits for icmp traffic.
  ```

  Next Available Option:

  - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**

if-ip

- show ip ospf interface *IP-ADDR*

  ```
  Specify IP address of the interface for which to show detailed information.
  ```

- show ip rip interface *IP-ADDR*

  ```
  Specify IP address of the interface for which to show detailed information.
  ```

igmp

- show igmp

  ```
  Usage: show igmp [...]

  Description: Show global switch IGMP configuration parameters.
               To get a list of all possible parameters use 'show igmp ?'.
  ```

  Next Available Option:

  - **delayed-flush** -- Shows switch-wide IGMP delayed flush value**(p. 467)**

- show ip igmp

  ```
  Usage: show ip igmp [config|group IP-ADDR|VLAN-ID [config]]

  Description: Invoked without any parameters, shows per-VLAN IGMP status,
               or, if VLANs are disabled displays the global IGMP status.
               When followed by the 'config' keyword, shows IGMP global
               configuration information. VLAN-ID can be used to get
               operational and configuration information for a particular
               VLAN, if VLAN support is enabled. The 'group' keyword can be
               used to show a list of ports where a particular multicast group
               is registered.
  ```

  Next Available Options:

  - **vlan** -- Show IGMP operational information for the VLAN specified. (VLAN-ID) **(p. 518)**
  - **config** -- Show IGMP configuration information.**(p. 462)**
  - **group** -- Show ports the specified multicast group address is registered on. (IP-ADDR) **(p. 473)**

igmp-proxy

- show igmp-proxy

```
Usage: show igmp-proxy <entries|domains|vlans>

Description: Show active/configured IGMP proxy forwarder information.
             When followed by the 'entries' keyword, shows all currently
             active IGMP proxy entries. The 'domains' keyword can be
             used to show all the currently configured IGMP proxy
             domains. The 'vlans' keyword can be used to show all the
             VLANs currently associated with IGMP proxy domains.
```

Next Available Options:

- **entries** -- Show all the currently active IGMP proxy entries.**(p. 470)**
- **domains** -- Show all the currently configured IGMP proxy domains.**(p. 469)**
- **vlans** -- Show all the VLANs currently associated with IGMP proxy domains.**(p. 521)**

INDEX

- show filter *INTEGER*

```
Show detailed information for the filter identified by the INDEX.
The indices are displayed by the 'show filter' command.
```

info

- show lldp info

```
Usage: show lldp info <local-device | remote device> [PORT-LIST]

Description: Show LLDP information about the remote or local device.
   o [ethernet] PORT-LIST - Show local or remote device information
                            for the specified ports.
```

Next Available Options:

- **remote-device** -- Show LLDP remote device information.**(p. 502)**
- **local-device** -- Show LLDP local device information.**(p. 486)**

information

- show system information

```
Usage: show system information

Description: Show global configured and operational system parameters.
```

instance

- show spanning-tree *[ETHERNET] PORT-LIST* config instance

```
Show the spanning tree instance information.
```

Next Available Options:

- **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 483)**

  - **MSTID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 491)**

- show spanning-tree *[ETHERNET] PORT-LIST* instance

  ```
  Show spanning tree instance status information.
  ```

  Next Available Options:
  - **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 483)**
  - **MSTID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 491)**

- show spanning-tree config instance

  ```
  Show the spanning tree instance information.
  ```

  Next Available Options:
  - **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 483)**
  - **MSTID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 491)**

- show spanning-tree instance

  ```
  Show the spanning tree instance information.
  ```

  Next Available Options:
  - **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 483)**
  - **MSTID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 491)**

- show spanning-tree pending instance

  ```
  Show multiple spanning tree instance pending configuration information.
  ```

  Next Available Options:
  - **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 483)**
  - **MSTID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 491)**

- show spanning-tree debug-counters instance *< 0 to 16 >*

  ```
  Show spanning tree instance debug counters information.
  ```

  Range: < 0 to 16 >

  Next Available Option:
  - **ports** -- Show spanning tree port(s) debug counters information. ([ethernet] PORT-LIST) **(p. 498)**

- show spanning-tree debug-counters ports *[ETHERNET] PORT-LIST* instance *< 0 to 16 >*

  ```
  Show spanning tree instance debug counters information.
  ```

  Range: < 0 to 16 >

instrumentation

- show instrumentation

```
Usage: show instrumentation

Description: Show internal version-dependant counters for debugging.
This data is for factory troubleshooting purposes.  The data displayed
is dependent on which version of code is running.

Data is maintained for the current 5 minutes, hour, and day.  At the end of
every 5 minutes, hour, or day, averages and min/max values are calculated
and the current interval's data is copied to the previous interval's data.
For example, the previous day's data is updated at midnight local time. The
previous hour's data is updated on the hour.

There are many situations in which data is not yet available, or data is
not maintained.  In this case, an asterisk is displayed.  It is never an
error condition.
```

Next Available Option:

- **monitor** -- Show latest values for monitored parameters**(p. 489)**

- show tech instrumentation

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

interface

- show ip ospf interface

```
Usage: show ip ospf interface [IP-ADDR|vlan VLAN-ID]

Description: Show OSPF interfaces' information. Invoked without
             parameters shows all OSPF interfaces configured. If the
             'IP-ADDR' or the VLAN is specified detailed information
             for the interface determined through the parameter is shown.
```

Next Available Options:

- **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 518)**
- **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 476)**

- show ip rip interface

```
Usage: show ip rip interface [IP-ADDR|vlan VLAN-ID]

Description: Show RIP interfaces' information. Invoked without
             parameters shows all RIP interfaces configured. If the
             'IP-ADDR' or the VLAN is specified detailed information
             for the interface determined through the parameter is shown.
```

Next Available Options:

- **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 518)**
- **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 476)**

- show ip mroute interface

```
Usage: show ip mroute interface [VLAN-ID]

Description: Show IP multicast routing interfaces' information. Invoked
             without parameters shows all IP multicast routing interfaces.
             If the VLAN-ID is specified then detailed information for the
             specified interface is shown.
```

Next Available Option:

- **VLAN-ID** -- Specify the VLAN ID of the IP multicast routing interface to show. (VLAN-ID) **(p. 520)**

- show ip pim interface

```
Usage: show ip pim interface [VLAN-ID]

Description: Show PIM interface information. Invoked without parameters
             shows all enabled PIM routing interfaces. If the VLAN-ID is
             specified then detailed information for the specified interface
             is shown.
```

Next Available Option:

- **VLAN-ID** -- Specify the VLAN ID of the PIM interface to show. (VLAN-ID) **(p. 520)**

interfaces

- show interfaces

```
Usage: show interfaces [config|brief|[ethernet] PORT-LIST|port-utilization]

Description: Show port configuration and status information.

     o config    - Show configuration information.
     o brief      - Show the ports' operational parameters.
     o [ethernet] PORT-LIST - Show summary of network traffic
                   handled by the ports.
     o port-utilization     - Show the ports' bandwidth-utilization.
```

Next Available Options:

- **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 496)**
- **config** -- Show configuration information**(p. 462)**
- **brief** -- Show the ports' operational parameters**(p. 458)**
- **port-utilization** -- Show the ports' bandwidth-utilization**(p. 498)**

intrusion-log

- show port-security intrusion-log

```
Show the intrusion log records.
```

ip

- show ip

```
Usage: show ip [...]

Description: Show the device IP configuration. Invoked without parameters
             shows IP configuration for the switch or all VLANs. When
             followed by a parameter displays information for a particular
             IP protocol or feature. To get a list of all possible
             parameters use 'show ip ?'.
```

Next Available Options:

- **authorized-managers** -- Show IPV4 addresses allowed to manage the switch**(p. 455)**
- **dns** -- Show configured DNS server IP addresses on the switch**(p. 469)**
- **client-public-key** -- Show currently loaded public keys for authorized clients (NUMBER) **(p. 459)**
- **helper-address** -- Show DHCP servers where DHCP requests received by the switch are to be forwarded**(p. 475)**
- **forward-protocol** -- Show server addresses where broadcast requests received by the switch are to be forwarded based on configured port**(p. 472)**
- **icmp** -- Show ICMP Rate Limiting settings**(p. 476)**
- **host-public-key** -- Display the SSH host RSA public key (NUMBER) **(p. 475)**
- **igmp** -- Invoked without any parameters, shows per-VLAN IGMP status, or, if VLANs are disabled displays the global IGMP status**(p. 476)**
- **irdp** -- Show IRDP (ICMP Router Discovery Protocol) settings**(p. 483)**
- **ospf** -- Show OSPF operational and configuration information**(p. 493)**
- **rip** -- Show RIP operational and configuration information**(p. 503)**
- **route** -- Show the IP routing table**(p. 504)**
- **ssh** -- Show both current SSH configuration and the status of active connections**(p. 509)**
- **mroute** -- Show IP multicast routing table**(p. 490)**
- **pim** -- Show PIM protocol operational and configuration information**(p. 495)**

- show rate-limit ip

```
ip help
```

Next Available Option:

- **access-group** -- access-group**(p. 451)**

ip-addr

- show ip route *IP-ADDR*

```
Destination IP address to display the routes to.
```

IP-ADDR

- show ip mroute *IP-ADDR*

```
Usage: show ip mroute [GRP-ADDR SRC-ADDR]

Description: Show detailed information for the specified entry from the IP
             multicast routing table. GRP-ADDR is the IP multicast group
             address and SRC-ADDR is the source IP address of the entry.
```

Next Available Option:

- **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 481)**

- show ip mroute *IP-ADDR IP-ADDR*

  ```
  Specify the source IP address of the MRT entry.
  ```

- show ip pim mroute *IP-ADDR*

  ```
  Specify the IP multicast group address of the MRT entry.
  ```

  Next Available Option:
  - **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 481)**

- show ip pim mroute *IP-ADDR IP-ADDR*

  ```
  Specify the source IP address of the MRT entry.
  ```

- show ip pim neighbor *IP-ADDR*

  ```
  Specify the IP address of the PIM neighbor to show.
  ```

ip-recv-mac-address

- show ip-recv-mac-address

  ```
  Show VLAN L3-Mac-Address table.
  ```

ipv6

- show ipv6

  ```
  Usage: show ipv6

  Description: Show the device IPv6 configuration. Invoked without parameters
               shows IPv6 configuration for the switch or all VLANs. When
               followed by a parameter displays information for a particular
               IPv6 protocol or feature. To get a list of all possible
               parameters use 'show ipv6 ?'.
  ```

  Next Available Options:
  - **vlan** -- Show IPv6 status information for all VLANs**(p. 518)**
  - **routers** -- Show the IPv6 Router table entries**(p. 505)**
  - **route** -- Show the IPv6 routing table**(p. 504)**
  - **mld** -- Invoked without any parameters, shows per-VLAN MLD status, or, if VLANs are disabled displays the global MLD status**(p. 489)**
  - **neighbors** -- Displays information on the IPv6 neighbor discovery cache**(p. 492)**
  - **authorized-managers** -- Show IPV6 addresses allowed to manage the switch**(p. 455)**

ipv6-addr

- show ipv6 route *IPV6-ADDR*

  ```
  Destination IPv6 address to display the routes to.
  ```

- show ipv6 mld vlan *VLAN-ID* group *IPV6-ADDR*

  ```
  Show MLD VLAN group address information.
  ```

irdp

- show ip irdp

```
Usage: show ip irdp

Description: Show IRDP (ICMP Router Discovery Protocol) settings.
```

ist

- show spanning-tree *[ETHERNET] PORT-LIST* config instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

- show spanning-tree *[ETHERNET] PORT-LIST* instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:

- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 467)**

- show spanning-tree config instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

- show spanning-tree instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:

- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 467)**

- show spanning-tree pending instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

- show spanning-tree root-history ist

```
Show IST Regional Root changes history.
```

jumbos

- show jumbos

```
Usage: show max-frame-size

Description: Show the untagged Max frame size for the switch.
             This value will be effective only when Jumbo is
             enabled.
```

key-chain

- show key-chain

```
Usage: show key-chain [CHAN-NAME-STR]

Description: Display key chains. The command displays a list of key chains
             configured. If a key chain name is specified the command shows
```

```
                the chain keys and information of routing protocols configured
                to use the chain.
```

Next Available Option:

- **CHAIN-NAME** -- Show the chain detailed information. (ASCII-STR) **(p. 459)**

keyfile

- show crypto client-public-key *< manager | operator >*

```
Choose to display manager or operator keys.
```

Supported Values:

- **manager** -- Select manager public keys.
- **operator** -- Select operator public keys.

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 457)**
- **fingerprint** -- Display hexadecimal hash.**(p. 472)**
- **keylist** -- Select keys to display (comma-delimited list). (ASCII-STR) **(p. 484)**

keylist

- show crypto client-public-key *< manager | operator > KEYLIST*

```
Select keys to display (comma-delimited list).
```

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 457)**
- **fingerprint** -- Display hexadecimal hash.**(p. 472)**

lacp

- show lacp

```
Usage: show lacp

Description: Show status of LACP trunks.
```

learned

- show ip pim rp-set learned

```
Show RP-Set information learned from the BSR.
```

licenses

- show licenses

```
Usage: show licenses [uninstalled]

Description: Display license status for premium features.  Use 'uninstalled'
             to display the uninstall verification key for features which
             have been uninstalled.
```

Next Available Option:

- **uninstalled** -- Display verification key for features which have been uninstalled. **(p. 516)**

link-keepalive

- show link-keepalive

```
Usage: show link-keepalive [statistics]

Description: show link-keepalive information on the switch.
             'show link-keepalive' command displays all the ports that are
             enabled for link-keepalive. 'show link-keepalive statistics'
             command displays detailed statistics like UDLD packets sent,
             UDLD packets received etc for all link-keepalive enabled ports.
```

Next Available Option:

- **statistics** -- show detailed statistics for all link-keepalive enabled ports.**(p. 510)**

link-state

- show ip ospf link-state

```
Usage: show ip ospf link-state [OSPF-AREA-ID] [status|advertise]

Description: Show all Link State Advertisements from throughout
             the areas to which the device is attached.
             The 'status' keyword is optional and does not affect the
             command output. If the 'advertise' is specified, each LSA
             is shown as a stream of bytes in hexadecimal notation.
```

Next Available Options:

- **area-id** -- Show LSAs for the specified area only. (OSPF-AREA-ID) **(p. 454)**
- **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation.**(p. 452)**
- **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 485)**
- **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 505)**
- **sequence-number** -- Show LSAs with the specified sequence number only.**(p. 506)**
- **status** -- The keyword is optional and can be omitted.**(p. 511)**
- **type** < router | network | summary | ... > -- Show LSAs of the specified type only.**(p. 515)**

link-state-id

- show ip ospf external-link-state link-state-id *IP-ADDR*

```
Show LSAs with the specified ID only.
```

- show ip ospf link-state link-state-id *IP-ADDR*

```
Show LSAs with the specified ID only.
```

lldp

- show lldp

```
Usage: show lldp ...
```

```
Description: Show various LLDP settings. Use 'show lldp ?' for the
             list of all possible options.
```

Next Available Options:

- **config** -- Show LLDP configuration information**(p. 462)**
- **info** -- Show LLDP information about the remote or local device**(p. 477)**
- **stats** -- Show LLDP statistics**(p. 511)**
- **auto-provision** -- Show LLDP auto-provision related info for radio-ports**(p. 456)**

local

- show ip pim bsr local

```
Show local Candidate-BSR configuration information.
```

local-device

- show lldp info local-device

```
Show LLDP local device information.
```

Next Available Option:

- **port-list** -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) **(p. 496)**

lockout-mac

- show lockout-mac

```
Usage: show lockout-mac

Description: Show the MAC addresses that have been locked out
             of the network.
```

logging

- show logging

```
Usage: show logging [-a|-r|-m|-p|-w|-i|-d|substring ...]

Description: Display log events.
             -a - Instructs the switch to display all recorded log
             events, which includes events from previous boot cycles.
             -r - Instructs the switch to display recorded
             log events in reverse order (most recent first).
             substring - Instructs the switch to display
             only those events that match the substring.

             The remaining event class options (listed below in
             order of severity - lowest severity first) confine
             output to event clases of equal or higher severity
             -d - Debug
             -i - Informative
             -w - Warnings
             -p - Performance
             -m - Major
             Only one of options -d,-i,-w,-p and -m may be specified.
             The -a, -r, and substring options may be used in
             combination with an event class option.
```

Next Available Options:

- **option** -- Filter events shown. See 'show logging help' for details. (ASCII-STR) **(p. 493)**
- **-a** -- Display all log events, including those from previous boot cycles.**(p. 451)**
- **-r** -- Display log events in reverse order (most recent first).**(p. 500)**
- **event_class** < -M | -P | -W | ... > -- Specify substring to match in log entry. See 'log help' for details.**(p. 470)**

loop-protect

- show loop-protect

```
Usage: show loop-protect [ethernet] PORT-LIST
Description: Show loop protection status. if no PORT-LIST is specified, then
             information is shown only for the ports that have loop protection
             enabled.
```

Next Available Option:

- **port-list** -- Show loop protection summary for ports. ([ethernet] PORT-LIST) **(p. 496)**

MAC

- show mac-address *MAC-ADDR*

```
Show port the specified MAC address is located on.
```

mac-address

- show mac-address

```
Usage: show mac-address [[ethernet] PORT-LIST|vlan VLAN-ID|MAC-ADDR]

Description: Show MAC addresses the switch has learned.
             You can display addresses learned on a particular port,
             a PORT-LIST, a VLAN-ID, or a particular MAC address.
```

Next Available Options:

- **address-table-port** -- Show MAC addresses learned on the specified ports. ([ethernet] PORT-LIST) **(p. 452)**
- **vlan** -- Show MAC addresses learned on the specified VLAN. (VLAN-ID) **(p. 518)**
- **MAC** -- Show port the specified MAC address is located on. (MAC-ADDR) **(p. 487)**

mac-based

- show port-access mac-based

```
Usage: show port-access [PORT-LIST] mac-based
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based [PORT-LIST]
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based config [PORT-LIST] [auth-server|detail]
```

```
Description: Show MAC Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
             of MAC Authentication is shown.
             If 'auth-server' keyword has been specified then the
             authentication server-related configuration items are shown.
             If PORT-LIST and 'detail' keyword has been specified then the
             detailed configuration of MAC Authentication for the specified
             ports is shown.
             If 'clients' keyword has been specified then the connected MAC
             address information is shown.
```

Next Available Options:

- -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
- **config** -- Show the current configuration of MAC Authentication.**(p. 462)**
- **clients** -- Show the connected MAC address information.**(p. 460)**

- show port-access *[ETHERNET] PORT-LIST* mac-based

```
Usage: show port-access [PORT-LIST] mac-based
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based [PORT-LIST]
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based config [PORT-LIST] [auth-server|detail]

Description: Show MAC Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
             of MAC Authentication is shown.
             If 'auth-server' keyword has been specified then the
             authentication server-related configuration items are shown.
             If PORT-LIST and 'detail' keyword has been specified then the
             detailed configuration of MAC Authentication for the specified
             ports is shown.
             If 'clients' keyword has been specified then the connected MAC
             address information is shown.
```

Next Available Options:

- **config** -- Show the current configuration of MAC Authentication.**(p. 462)**
- **clients** -- Show the connected MAC address information.**(p. 460)**

management

- show management

```
Usage: show management

Description: Show the switch's addresses available for management
             and the time server if the switch uses one.
```

mesh

- show mesh

```
Usage: show mesh

Description: Show the switch mesh information such as mesh
             ports, adjacent switches and their peer ports.
```

- show tech mesh

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

mirror_session_id

- show monitor *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

mld

- show ipv6 mld

```
Usage: show ipv6 mld [config|group IPV6-ADDR|VLAN-ID [config]]

Description: Invoked without any parameters, shows per-VLAN MLD status,
             or, if VLANs are disabled displays the global MLD status.
             When followed by the 'config' keyword, shows MLD global
             configuration information. VLAN-ID can be used to get
             operational and configuration information for a particular
             VLAN, if VLAN support is enabled. The 'group' keyword can be
             used to show a list of ports where a particular multicast group
             is registered.
```

Next Available Options:

- **vlan** -- Show MLD VLAN information.**(p. 518)**
- **config** -- Show MLD configuration information.**(p. 462)**
- **statistics** -- Show MLD statistics.**(p. 510)**

modules

- show modules

```
Usage: show modules

Description: Show installed modules information
```

monitor

- show instrumentation monitor

```
Usage: show instrumentation monitor

Description: Show latest values for monitored parameters.
The data displayed is dependent on which version of code is running.

Data is maintained for the current 5 minutes, hour, and day.  At the end of
```

```
every 5 minutes, hour, or day, averages and min/max values are calculated
and the current interval's data is copied to the previous interval's data.
For example, the previous day's data is updated at midnight local time. The
previous hour's data is updated on the hour.

There are many situations in which data is not yet available, or data is
not maintained.  In this case, an asterisk is displayed.  It is never an
error condition.
```

Next Available Option:

- **configuration** -- show configured thresholds for monitored parameters**(p. 465)**

- show monitor

```
Usage: show monitor

Description: Show the switch network monitoring status and
             configuration, if network monitoring is enabled.
```

Next Available Options:

- **mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 489)**
- **name** -- Mirror destination name.**(p. 492)**
- **endpoint** -- Remote mirroring destination configuration.**(p. 470)**

motd

- show banner motd

```
Usage: show banner motd

Description: show the configured banner text.
```

mroute

- show ip mroute

```
Usage: show ip mroute [command]

Description: Show IP multicast routing table. The 'command' can be used to
             obtain more detailed information of the IP multicast routing
             functionality. Use 'show ip mroute ?' to get a list of all
             possible commands.
```

Next Available Options:

- **IP-ADDR** -- Show detailed information for the specified entry from the IP multicast routing table (IP-ADDR) **(p. 481)**
- **interface** -- Show IP multicast routing interfaces' information**(p. 479)**

- show ip pim mroute

```
Usage: show ip pim mroute [GRP-ADDR SRC-ADDR]

Description: Show PIM-specific information from the IP multicast routing
             table. Invoked without parameters shows all PIM entries from
             the IP MRT. If multicast group address and source address are
```

```
specified then detailed information for the specified entry is
shown.
```

Next Available Option:

- **IP-ADDR** -- Specify the IP multicast group address of the MRT entry. (IP-ADDR) **(p. 481)**

mst-config

- show spanning-tree mst-config

  ```
  Show multiple spanning tree region configuration.
  ```

- show spanning-tree pending mst-config

  ```
  Show multiple spanning tree pending region configuration.
  ```

msti

- show spanning-tree root-history msti *< 1 to 16 >*

  ```
  Show MSTI Regional Root changes history.
  ```

  Range: < 1 to 16 >

MSTID

- show spanning-tree *[ETHERNET] PORT-LIST* config instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

- show spanning-tree *[ETHERNET] PORT-LIST* instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

  Next Available Option:

  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 467)**

- show spanning-tree config instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

- show spanning-tree instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

  Next Available Option:

  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 467)**

- show spanning-tree pending instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

Range: < 1 to 16 >

name

- show monitor name

```
Mirror destination name.
```

- show name

```
Usage: show name [[ethernet] PORT-LIST]

Description: Show names assigned to the ports. If the PORT-LIST is not
             specified the default is to list all of the ports.
```

Next Available Option:

- **port-list** -- Show names assigned to the ports ([ethernet] PORT-LIST) **(p. 496)**

neighbor

- show ip ospf neighbor

```
Usage: show ip ospf neighbor [IP-ADDR]

Description: Show all OSPF neighbors in the locality of of the
             device. The 'IP-ADDR' can be specified to retrieve
             detailed information for the specific neighbor only.
```

Next Available Option:

- **neighbor-ip** -- (IP-ADDR) **(p. 492)**

- show ip pim neighbor

```
Usage: show ip pim neighbor [IP-ADDR]

Description: Show PIM neighbor information. Invoked without parameters
             shows all PIM neighbors of this device. If the IP-ADDR is
             specified then detailed information for the specified neighbor
             is shown.
```

Next Available Option:

- **IP-ADDR** -- Specify the IP address of the PIM neighbor to show. (IP-ADDR) **(p. 481)**

neighbor-ip

- show ip ospf neighbor *IP-ADDR*

neighbors

- show cdp neighbors

```
Show CDP neighbors. See 'show cdp help' for details.
```

Next Available Options:

- **neighbors-port** -- Show CDP neighbors on specified port only. ([ethernet] PORT-NUM) **(p. 493)**
- **detail** -- Show neighbor information field-per-line instead of shortened table format.**(p. 467)**

- show ipv6 neighbors

  ```
  Displays information on the IPv6 neighbor discovery cache
  ```

  Next Available Option:
  - **vlan** -- Displays information on the IPv6 neighbor discovery cache**(p. 518)**

neighbors-port

- show cdp neighbors *[ETHERNET] PORT-NUM*

  ```
  Show CDP neighbors on specified port only.
  ```

notify

- show snmpv3 notify

  ```
  Show SNMPv3 notification table.
  ```

  Next Available Option:
  - **NOTIFY-NAME** -- Show a specific notification entry. (ASCII-STR) **(p. 493)**

NOTIFY-NAME

- show snmpv3 notify *NOTIFY-NAME*

  ```
  Show a specific notification entry.
  ```

only

- show snmpv3 only

  ```
  Show SNMP message reception policy.
  ```

option

- show logging *OPTION*

  ```
  Filter events shown. See 'show logging help' for details.
  ```

ospf

- show ip ospf

  ```
  Usage: show ip ospf [command]

  Description: Show OSPF operational and configuration information.
               The 'command' can be used to obtain more detailed information
               of the protocol functionality. Use 'show ip ospf ?' to get a
               list of all possible commands.
  ```

  Next Available Options:
  - **general** -- Show OSPF basic configuration and operational information**(p. 473)**
  - **area** -- Show OSPF areas configured on the device**(p. 453)**
  - **external-link-state** -- Show the Link State Advertisements from throughout the areas to which the device is attached**(p. 471)**

- **interface** -- Show OSPF interfaces' information**(p. 479)**
- **link-state** -- Show all Link State Advertisements from throughout the areas to which the device is attached**(p. 485)**
- **neighbor** -- Show all OSPF neighbors in the locality of of the device**(p. 492)**
- **redistribute** -- List protocols which are being redistributed into OSPF**(p. 501)**
- **restrict** -- List routes which will not be redistributed via OSPF**(p. 503)**
- **traps** -- Show OSPF traps enabled on the device**(p. 515)**
- **virtual-neighbor** -- Show all virtual neighbors of the device**(p. 518)**
- **virtual-link** -- Show status of all OSPF virtual links configured**(p. 517)**

output

- show bandwidth output

```
Show outbound guaranteed minimum bandwidth.
```

Next Available Option:

- **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 496)**

PARAM-NAME

- show snmpv3 params *PARAM-NAME*

```
Show a specific Target Parameter entry.
```

params

- show snmpv3 params

```
Show SNMPv3 Target Parameters table.
```

Next Available Option:

- **PARAM-NAME** -- Show a specific Target Parameter entry. (ASCII-STR) **(p. 494)**

peer

- show ip rip peer

```
Usage: show ip rip peer [IP-ADDR]

Description: Show RIP peers. Invoked without parameters shows all RIP
             peers of the device. If 'IP-ADDR' is specified only
             the peer having the address is displayed.
```

Next Available Option:

- **peer-ip** -- Specify IP address of the RIP peer to show. (IP-ADDR) **(p. 494)**

peer-ip

- show ip rip peer *IP-ADDR*

```
Specify IP address of the RIP peer to show.
```

pending

- show ip pim pending

```
Show (*,G) and (S,G) Join Pending Information.
```

- show spanning-tree pending

```
Usage: show spanning-tree pending ...

Description: Show spanning tree pending configuration.
             Use 'show spanning-tree pending ?' to see a list of all
             available options.
```

Next Available Options:

- **mst-config** -- Show multiple spanning tree pending region configuration.**(p. 491)**
- **instance** -- Show multiple spanning tree instance pending configuration information.**(p. 477)**

pim

- show ip pim

```
Usage: show ip pim [command]

Description: Show PIM protocol operational and configuration information.
             The 'command' can be used to obtain more detailed information
             of the protocol functionality. Use 'show ip pim ?' to get a
             list of all possible commands.
```

Next Available Options:

- **mroute** -- Show PIM-specific information from the IP multicast routing table**(p. 490)**
- **interface** -- Show PIM interface information**(p. 479)**
- **neighbor** -- Show PIM neighbor information**(p. 492)**
- **bsr** -- Show Bootstrap Router information**(p. 458)**
- **rp-candidate** -- Show Candidate-RP operational and configuration information**(p. 505)**
- **rp-set** -- Show RP-Set information available on the router**(p. 505)**
- **rp-pending** -- Show (*,*,RP) Join Pending Information. **(p. 505)**
- **pending** -- Show (*,G) and (S,G) Join Pending Information. **(p. 495)**

port-access

- show port-access

```
Usage: show port-access <authenticator [...] | supplicant [...]>

Description: Show 802.1X (Port Based Network Access) supplicant or
             authenticator current status and configuration.
```

Next Available Options:

- **authenticator** -- Show 802.1X authenticator statistics and configuration. **(p. 455)**
- **supplicant** -- Show 802.1X supplicant statistics and configuration. **(p. 512)**
- **mac-based** -- Show MAC Authentication statistics and configuration**(p. 487)**
- **web-based** -- Show Web Authentication statistics and configuration**(p. 522)**
- -- Show Web/MAC Authentication statistics and configuration ([ethernet] PORT-LIST) **(p. 449)**
- **config** -- Show status of 802.1X, Web Auth, and MAC Auth configurations. **(p. 462)**

port-list

- show interfaces *[ETHERNET] PORT-LIST*

  ```
  Usage: show interfaces [ethernet] PORT-LIST

  Description: Show summary of network traffic handled by the ports.
  ```

  Next Available Option:
  - **hc** -- Show summary of network traffic handled by the ports**(p. 474)**

- show interfaces brief *[ETHERNET] PORT-LIST*

  ```
  Usage: show interfaces [ethernet] PORT-LIST

  Description: Show summary of network traffic handled by the ports.
  ```

- show lldp config *[ETHERNET] PORT-LIST*

  ```
  Specify the port or list of ports.
  ```

- show lldp info remote-device *[ETHERNET] PORT-LIST*

  ```
  Show remote or local device information for the
                                     specified ports.
  ```

- show lldp info local-device *[ETHERNET] PORT-LIST*

  ```
  Show remote or local device information for the
                                     specified ports.
  ```

- show lldp stats *[ETHERNET] PORT-LIST*

  ```
  Specify the port or list of ports.
  ```

- show loop-protect *[ETHERNET] PORT-LIST*

  ```
  Show loop protection summary for ports.
  ```

- show name *[ETHERNET] PORT-LIST*

  ```
  Usage: show name [[ethernet] PORT-LIST]

  Description: Show names assigned to the ports. If the PORT-LIST is not
               specified the default is to list all of the ports.
  ```

- show port-security *[ETHERNET] PORT-LIST*

  ```
  Usage: show port-security [intrusion-log|[ethernet] PORT-LIST]

  Description: Show a table describing port security settings.

      o intrusion-log - Show the intrusion log records.
      o PORT-LIST     - Show detailed information on particular ports in the
                        PORT-LIST specified.
  ```

- show power-over-ethernet *[ETHERNET] PORT-LIST*

```
Usage: show power-over-ethernet [ethernet] PORT-LIST

Description: Show the ports' poe status.
```

- show power-over-ethernet brief *[ETHERNET] PORT-LIST*

```
Usage: show power-over-ethernet [ethernet] PORT-LIST

Description: Show the ports' poe status.
```

- show bandwidth output *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show rate-limit icmp *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show rate-limit all *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show rate-limit ip access-group *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show sflow *< 1 to 3 >* sampling-polling *[ETHERNET] PORT-LIST*

```
Displays information about sampling and polling.
```

- show spanning-tree *[ETHERNET] PORT-LIST*

```
Limit the port information printed to the set of the specified ports.
```

Next Available Options:

- **config** -- Show spanning tree configuration information.**(p. 462)**
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 467)**
- **instance** -- Show spanning tree instance status information.**(p. 477)**

- show spanning-tree bpdu-protection *[ETHERNET] PORT-LIST*

```
Limit the port information printed to the set of the specified ports.
```

- show spanning-tree pvst-filter *[ETHERNET] PORT-LIST*

```
Limit the port information printed to the set of the specified ports.
```

- show spanning-tree pvst-protection *[ETHERNET] PORT-LIST*

```
Limit the port information printed to the set of the specified ports.
```

- show trunks *[ETHERNET] PORT-LIST*

```
Show the trunk information only for the ports specified.
```

port-priority

- show qos port-priority

```
Usage: show qos port-priority

Description: Show the port-based priority table.
```

ports

- show access-list ports *[ETHERNET] PORT-LIST*

  ```
  Show ACLs applied to the specified ports.
  ```

- show spanning-tree debug-counters instance *< 0 to 16 >* ports *[ETHERNET] PORT-LIST*

  ```
  Show spanning tree port(s) debug counters information.
  ```

- show spanning-tree debug-counters ports *[ETHERNET] PORT-LIST*

  ```
  Show spanning tree port(s) debug counters information.
  ```

  Next Available Option:
  - **instance** < 0 to 16 > -- Show spanning tree instance debug counters information. (NUMBER) **(p. 477)**

- show vlans ports *[ETHERNET] PORT-LIST*

  ```
  Show VLANs that have at least one port from the 'PORT-LIST' as a member.
  ```

  Next Available Option:
  - **detail** -- Display more info for each port from the 'PORT-LIST' separately.**(p. 467)**

- show svlans ports *[ETHERNET] PORT-LIST*

  ```
  Show VLANs that have at least one port from the 'PORT-LIST' as a member.
  ```

  Next Available Option:
  - **detail** -- Display more info for each port from the 'PORT-LIST' separately.**(p. 467)**

port-security

- show port-security

  ```
  Usage: show port-security [intrusion-log|[ethernet] PORT-LIST]

  Description: Show a table describing port security settings.

      o intrusion-log - Show the intrusion log records.
      o PORT-LIST     - Show detailed information on particular ports in the
                        PORT-LIST specified.
  ```

  Next Available Options:
  - **port-list** -- Show a table describing port security settings ([ethernet] PORT-LIST) **(p. 496)**
  - **intrusion-log** -- Show the intrusion log records.**(p. 480)**

port-utilization

- show interfaces port-utilization

```
Usage: show interfaces port-utilization

Description: Show the ports' bandwidth-utilization.
```

power-over-ethernet

- show power-over-ethernet

```
Usage: show power-over-ethernet [brief|[ethernet] PORT-LIST]

Description: Show port poe configuration and status information.

     o brief      - Show summary of poe status.
     o [ethernet] PORT-LIST - Show the ports' power status.
```

Next Available Options:

- **port-list** -- Show the ports' poe status ([ethernet] PORT-LIST) **(p. 496)**
- **brief** -- Show summary of poe status**(p. 458)**
- **slot** -- Show poe information of specified slot (SLOT-ID-RANGE) **(p. 507)**

power-supply

- show system power-supply

```
Usage: show system power-supply

Description: Show Chassis Power Supply info and settings.
```

protocol-priority

- show qos protocol-priority

```
Usage: show qos protocol

Description: Show the protocol priority.
```

pvst-filter

- show spanning-tree pvst-filter

```
Show spanning tree PVST filter status information.
```

Next Available Option:

- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**

pvst-protection

- show spanning-tree pvst-protection

```
Show spanning tree PVST protection status information.
```

Next Available Option:

- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**

qinq

- show qinq

```
Usage:  show qinq

Description:  show qinq configuration details.
```

qos

- show qos

```
Usage: show qos ...

Description: Show various QoS settings. Use 'show qos ?' for the
             list of all possible options.
```

Next Available Options:

- **device-priority** -- Show the device priority table (priority based on the IP addresses)**(p. 469)**
- **dscp-map** -- Show mappings between DSCP policy and 802.1p priority. **(p. 470)**
- **port-priority** -- Show the port-based priority table**(p. 497)**
- **protocol-priority** -- Show the protocol priority**(p. 499)**
- **tcp-udp-port-priority** -- Show TCP/UDP port priorities**(p. 513)**
- **type-of-service** -- Show QoS priorities based on IP Type-of-Service**(p. 516)**
- **vlan-priority** -- Show the VLAN-based priority table**(p. 521)**
- **resources** -- Show the qos resources**(p. 502)**
- **queue-config** -- Displays outbound port queues configuration information. **(p. 500)**

queue-config

- show qos queue-config

```
Displays outbound port queues configuration information.
```

-r

- show logging -r

```
Display log events in reverse order (most recent first).
```

radio-ports

- show wireless-services *SLOT-ID* radio-ports

```
Display radio-ports associated with a wireless-services module.
```

- show lldp auto-provision radio-ports

```
Show LLDP radio-ports information.
```

radius

- show access-list radius *[ETHERNET] PORT-LIST*

```
Display ACLs applied via RADIUS.
```

- show radius

```
Usage: show radius [authentication|accounting|dyn-authorization|host <IP-ADDR>]

Description: Show RADIUS status and statistics information. Invoked without
             parameters shows general RADIUS configuration for the switch.

    o authentication    - show RADIUS authentication statistics information.

    o accounting        - show RADIUS accounting statistics information.

    o dyn-authorization - show RADIUS dynamic authorization statistics
                          information.

    o host <IP-ADDR>    - show comprehensive statistics information for the
                          host.
```

Next Available Options:

- **authentication** -- Show RADIUS authentication statistics**(p. 454)**
- **accounting** -- Show RADIUS accounting statistics**(p. 452)**
- **dyn-authorization** -- Show RADIUS dynamic authorization statistics**(p. 470)**
- **host** -- Show statistics information for the RADIUS host (IP-ADDR) **(p. 475)**

rate-limit

- show rate-limit

```
Usage: show rate-limit <all|icmp> [PORT-LIST]

Description: Show rate limit maximum percentages. If PORT-LIST parameter is
             specified, information is shown only for the specified ports.

             Use 'all' to show limits applied to all traffic, or 'icmp' to
             show limits for ICMP traffic only.
```

Next Available Options:

- **icmp** -- Show only limits for icmp traffic.**(p. 476)**
- **all** -- Show limits for all traffic.**(p. 453)**
- **ip** -- ip help**(p. 480)**

receiver-index

- show sflow *< 1 to 3 >*

```
Select one of the three possible sFlow receiver tables.
```

Range: < 1 to 3 >

Next Available Options:

- **destination** -- Displays information about the receiver/collector/management-station to which the sampling-polling data is sent.**(p. 467)**
- **sampling-polling** -- Displays information about sampling and polling.**(p. 506)**

redistribute

- show ip ospf redistribute

```
Usage: show ip ospf redistribute

Description: List protocols which are being redistributed into OSPF.
```

- show ip rip redistribute

```
Usage: show ip rip redistribute

Description: List protocols which are being redistributed into RIP.
```

redundancy

- show redundancy

```
Usage: show redundancy

Description: Display redundant information for Management and Fabric Modules.
It displays the flash image last booted from, even if the boot set-default
command has been set to change the flash booted from on the next boot.
```

Example 1. Example of show redundancy Command

```
ProCurve(config)# show redundancy

  Settings
  --------
   Mgmt Redundancy : enabled

  Statistics
  ----------
   Failovers     : 0
   Last Failover :

Slot Module Description                            Status   SW Version Boot Image
---- --------------------------------------- -------- ---------- ----------
MM1  ProCurve J9092A Management Module 8200zl Active   K.12.30    Primary
MM2  ProCurve J9092A Management Module 8200zl Standby  K.12.30    Primary

FM1  ProCurve J9093A Fabric Module 8200zl     Enabled
FM2  ProCurve J9093A Fabric Module 8200zl     Enabled
```

remote-device

- show lldp info remote-device

```
Show LLDP remote device information.
```

Next Available Option:

- **port-list** -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) **(p. 496)**

resources

- show access-list resources

```
Display ACL Rules/Masks availability.
```

- show qos resources

```
Usage: show qos resources

Description: Show the qos resources.
```

restrict

- show ip ospf restrict

```
Usage: show ip ospf restrict

Description: List routes which will not be redistributed via OSPF.
```

- show ip rip restrict

```
Usage: show ip rip restrict

Description: List routes which will not be redistributed via RIP.
```

restricted-access

- show snmpv3 restricted-access

```
Show SNMPv1 and SNMPv2c access properties.
```

rip

- show ip rip

```
Usage: show ip rip [command]

Description: Show RIP operational and configuration information.
             The 'command' can be used to obtain more detailed information
             of the protocol functionality. Use 'show ip rip ?' to get a
             list of all possible commands.
```

Next Available Options:

- **general** -- Show RIP basic configuration and operational information**(p. 473)**
- **interface** -- Show RIP interfaces' information**(p. 479)**
- **peer** -- Show RIP peers**(p. 494)**
- **redistribute** -- List protocols which are being redistributed into RIP**(p. 501)**
- **restrict** -- List routes which will not be redistributed via RIP**(p. 503)**

rmon

- show rmon

```
Usage: show rmon statistics PORT-LIST

Description: Show detailed rmon statistics for the ports.

     o statistics PORT-LIST - Show statistics measured by the
                  probe for the ports.
```

Next Available Option:

- **statistics** -- Show RMON statistics for the ports ([ethernet] PORT-LIST) **(p. 510)**

root-history

- show spanning-tree root-history

```
Show spanning tree Root changes history information.
```

Next Available Options:

- **cst** -- Show CST Root changes history.**(p. 466)**
- **ist** -- Show IST Regional Root changes history.**(p. 483)**
- **msti** < 1 to 16 > -- Show MSTI Regional Root changes history. (NUMBER) **(p. 491)**

Example 2. Example of the show root-history Command

```
ProCurve(config)# show spanning-tree root-history ist

 Status and Counters - IST Regional Root Changes History

  MST Instance ID         : 0
  Root Changes Counter    : 1
  Current Root Bridge ID : 32768:001659-9d0f00

  Root Bridge ID      Date      Time
  ------------------- --------- ---------
  32768:001659-9d0f00 01/02/90 00:07:23
```

route

- show ip route

```
Usage: show ip route [IP-ADDR] [static|connected|rip|ospf]

Description: Show the IP routing table.
             The output may be restricted to a specific destination or
             type of route.
```

Next Available Options:

- **ip-addr** -- Destination IP address to display the routes to. (IP-ADDR) **(p. 481)**
- **type** < static | connected | rip | ... > -- Specify type of routes to display.**(p. 515)**

- show ipv6 route

```
Usage: show ipv6 route [IPV6-ADDR] [connected]

Description: Show the IPv6 routing table.
             The output may be restricted to a specific destination or
             type of route.
```

Next Available Options:

- **ipv6-addr** -- Destination IPv6 address to display the routes to. (IPV6-ADDR) **(p. 482)**
- **type** < connected > -- Specify type of routes to display.**(p. 515)**

- show tech route

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

router-id

- show ip ospf external-link-state router-id *IP-ADDR*

  ```
  Show LSAs with the specified Router ID only.
  ```

- show ip ospf link-state router-id *IP-ADDR*

  ```
  Show LSAs with the specified Router ID only.
  ```

routers

- show ipv6 routers

  ```
  Usage: show ipv6 routers vlan <VLANID>

  Description: Show the IPv6 Router table entries.
  ```

  Next Available Option:

  - **vlan** -- Show the IPv6 Router Table Entries for VLAN.**(p. 518)**

rp-candidate

- show ip pim rp-candidate

  ```
  Usage: show ip pim rp-candidate [config]

  Description: Show Candidate-RP operational and configuration information.
               When invoked without parameter shows current operational status
               of the Candidate-RP.
  ```

  Next Available Option:

  - **config** -- Show C-RP configuration information. **(p. 462)**

rp-pending

- show ip pim rp-pending

  ```
  Show (*,*,RP) Join Pending Information.
  ```

rp-set

- show ip pim rp-set

  ```
  Usage: show ip pim rp-set [static|learned]

  Description: Show RP-Set information available on the router.
               When invoked without parameters shows all statically configured
               and dynamically learned entries. If keyword 'static' is specified
               the information about statically configured entries is shown.
               If keyword 'learned' is specified the information learned from
               the BSR is shown.
  ```

  Next Available Options:

  - **static** -- Show statically configured RP-Set information. **(p. 510)**
  - **learned** -- Show RP-Set information learned from the BSR. **(p. 484)**

running-config

- show running-config

```
Usage: show running-config [status]

Description: Show the switch running configuration. If the status
             keyword is specified check if there are changes in running
             configuration not saved to startup configuration file.
```

Next Available Option:

- **status** -- Check if the running configuration differs from the statup configuration.**(p. 511)**

sampling-polling

- show sflow < *1 to 3* > sampling-polling

```
Displays information about sampling and polling.
```

Next Available Option:

- **port-list** -- Displays information about sampling and polling. ([ethernet] PORT-LIST) **(p. 496)**

sec-model

- show snmpv3 access-rights < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | *...* > sec-model

```
Set security model.
```

Next Available Options:

- **ver1-2c** < ver1 | ver2c > -- Configure SNMPv3 User entry.**(p. 516)**
- **ver3** -- SNMP version 3 security model.**(p. 517)**

- show snmpv3 group < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | *...* > user *USER* sec-model < *ver1* | *ver2c* | *ver3* >

```
Show a specific security model.
```

Supported Values:

- **ver1** -- SNMP version 1 security model.
- **ver2c** -- SNMP version v2c security model.
- **ver3** -- SNMP version 3 security model.

sequence-number

- show ip ospf external-link-state sequence-number *INTEGER*

```
Show LSAs with the specified sequence number only.
```

- show ip ospf link-state sequence-number *INTEGER*

```
Show LSAs with the specified sequence number only.
```

session-counters

- show port-access authenticator *[ETHERNET] PORT-LIST* session-counters

```
Show 802.1X current (or last if no current sessions open) sessions counters.
```

- show port-access authenticator session-counters

  ```
  Show 802.1X current (or last if no current sessions open) sessions counters.
  ```

- show port-access *[ETHERNET] PORT-LIST* authenticator session-counters

  ```
  Show 802.1X current (or last if no current sessions open) sessions counters.
  ```

sessions

- show accounting sessions

  ```
  Usage: show accounting sessions

  Description: Show accounting data for all active sessions.
  ```

sflow

- show sflow

  ```
  Usage: show sflow <agent | destination | all |
                    sampling-polling [ethernet] PORT-LIST>

  Description: Display information regarding the configuration,
               sampling, and polling with respect to 'sflow'.
  ```

  Next Available Options:

  - **agent** -- Displays read-only switch agent information: The agent address is normally the ip address of the first vlan configured.**(p. 453)**
  - **receiver-index** < 1 to 3 > -- Select one of the three possible sFlow receiver tables. (NUMBER) **(p. 501)**

slave_time

- show cpu slot *SLOT-ID-RANGE < 1 to 90 >*

  ```
  Time (seconds) over which to average CPU utilization.
  ```

  Range: < 1 to 90 >

slot

- show cpu slot *SLOT-ID-RANGE*

  ```
  Display module CPU statistics.
  ```

  Next Available Option:

  - **slave_time** < 1 to 90 > -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 507)**

- show power-over-ethernet brief slot *SLOT-ID-RANGE*

  ```
  Usage: show power-over-ethernet brief

  Description: Show summary of poe status.
  ```

- show power-over-ethernet slot *SLOT-ID-RANGE*

```
Usage: show power-over-ethernet [slot] <slotID>

Description: Show poe information of specified slot.
```

snmp-server

- show snmp-server

```
Usage: show snmp-server [COMMUNITY-STR]
       show snmp-server traps

Description: Display information on all SNMP communities, trap receivers and
             Snmp response/trap source-ip policy configured on the switch. If
             'COMMUNITY-STR' is specified, only information for that community
             is displayed.
```

Next Available Options:

- **traps** -- Show all configured traps.**(p. 515)**
- **community** -- Specify SNMP community to which to restrict the output. (ASCII-STR) **(p. 461)**

snmpv3

- show snmpv3

```
Show configuration of SNMPv3 features.
```

Next Available Options:

- **access-rights** -- Show information about access rights. **(p. 452)**
- **community** -- Show SNMPv3 Community table. **(p. 461)**
- **enable** -- Show SNMPv3 status. **(p. 470)**
- **engineid** -- Show switch's SNMP engineId. **(p. 470)**
- **group** -- Show SNMPv3 User to Group mappings. **(p. 473)**
- **notify** -- Show SNMPv3 notification table. **(p. 493)**
- **only** -- Show SNMP message reception policy. **(p. 493)**
- **params** -- Show SNMPv3 Target Parameters table. **(p. 494)**
- **restricted-access** -- Show SNMPv1 and SNMPv2c access properties. **(p. 503)**
- **targetaddress** -- Show SNMPv3 Target Address table. **(p. 513)**
- **user** -- Show SNMPv3 users. **(p. 516)**
- **view** -- Show views. **(p. 517)**

sntp

- show sntp

```
Usage: show sntp

Description: Show configured time protocol and servers.
```

source-port

- show filter source-port

```
Usage: show filter source-port
```

```
Description: Show a table of source-port filter names
             with the associated source ports and actions
```

spanning-tree

- show spanning-tree

```
Usage: show spanning-tree [[ethernet] PORT-LIST] [config|detail]
       show spanning-tree [[ethernet] PORT-LIST] instance <ist|INSTANCE-ID>
                          [detail]
       show spanning-tree [mst-config] |
                          [config [instance <ist|INSTANCE-ID>]] |
                          [root-history <cst|ist|msti <INSTANCE-ID>>] |
                          [debug-counters [instance <INSTANCE-ID>] |
                                          [ports <PORT_LIST>]]

Description: Show spanning tree information.
             When executed without parameters, the command shows spanning
             tree status information. If PORT-LIST is specified, the
             command shows spanning tree status information only for the
             ports listed. If the 'config' keyword is specified the spanning
             tree configuration information is shown. If the 'detail' keyword
             is specified, extended port, cost, and BPDU information is shown.
             The second and third forms of the command can be used to show
             MSTP specific information. Use the 'show spanning-tree ?'
             command to see all available parameters with description.
```

Next Available Options:

- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 496)**
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 467)**
- **config** -- Show spanning tree configuration information.**(p. 462)**
- **instance** -- Show the spanning tree instance information.**(p. 477)**
- **mst-config** -- Show multiple spanning tree region configuration.**(p. 491)**
- **pending** -- Show spanning tree pending configuration**(p. 495)**
- **root-history** -- Show spanning tree Root changes history information.**(p. 504)**
- **debug-counters** -- Show spanning tree debug counters information.**(p. 467)**
- **traps** -- Show spanning tree trap information.**(p. 515)**
- **bpdu-protection** -- Show spanning tree BPDU protection status information.**(p. 458)**
- **pvst-filter** -- Show spanning tree PVST filter status information.**(p. 499)**
- **pvst-protection** -- Show spanning tree PVST protection status information.**(p. 499)**

ssh

- show ip ssh

```
Usage: show ip ssh

Description: Show both current SSH configuration and the status of active
             connections.
```

stack

- show stack

```
Usage: show stack [candidates|view|all]
```

```
Description: Show the stack status of this switch. The 'candidate' and
             'view' commands are available on the stack commander only.

    o candidates - show the list of devices that are stack candidates.

    o view - show the list of devices that are stack members.

    o all - show information about all the stacks available on the LAN.
```

Next Available Options:

- **candidates** -- Show the list of devices that are stack candidates.**(p. 459)**
- **view** -- Show the list of devices that are stack members.**(p. 517)**
- **all** -- Show information about all the stacks available on the LAN.**(p. 453)**

static

- show ip pim rp-set static

```
Show statically configured RP-Set information.
```

static-mac

- show static-mac

```
Usage: show static-mac

Description: Show the locked-down MAC addresses in all vlans.
             The list is sorted by VLAN, then MAC address.
```

statistics

- show arp-protect statistics *VLAN-ID-RANGE*
- show ipv6 mld vlan *VLAN-ID* statistics

```
Show MLD VLAN statistics
```

- show ipv6 mld statistics

```
Show MLD statistics.
```

- show link-keepalive statistics

```
show detailed statistics for all link-keepalive enabled ports.
```

- show port-access authenticator *[ETHERNET] PORT-LIST* statistics

```
Show authentication sessions statistics for 802.1X authenticator.
```

- show port-access authenticator statistics

```
Show authentication sessions statistics for 802.1X authenticator.
```

- show port-access supplicant statistics

```
Show authentication sessions statistics for 802.1X supplicant.
```

- show port-access *[ETHERNET] PORT-LIST* authenticator statistics

```
Show authentication sessions statistics for 802.1X authenticator.
```

- show rmon statistics *[ETHERNET] PORT-LIST*

```
Usage: show rmon statistics PORT-LIST

Description: Show RMON statistics for the ports.
```

- show tech statistics

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

- show vrrp statistics

```
Usage: show vrrp statistics

Description: Show VRRP statistics information for the device.
```

Next Available Option:

- **global** -- Show global VRRP configuration information. **(p. 473)**

- show vrrp vlan *VLAN-ID* statistics

```
Show VRRP statistics information for the VLAN.
```

- show vrrp vlan *VLAN-ID* vrid *< 1 to 255 >* statistics

```
Show virtual router statistics information.
```

stats

- show dhcp-snooping stats

```
Display DHCP snooping events.
```

- show lldp stats

```
Usage: show lldp stats [[ethernet] PORT-LIST]

Description: Show LLDP statistics.
   o [ethernet] PORT-LIST - Show statistics for the specified ports .
```

Next Available Option:

- **port-list** -- Specify the port or list of ports. ([ethernet] PORT-LIST) **(p. 496)**

status

- show config status

```
Check if the running configuration differs from the statup configuration.
```

- show ip ospf external-link-state status

```
The keyword is optional and can be omitted.
```

- show ip ospf link-state status

```
The keyword is optional and can be omitted.
```

- show running-config status

```
Check if the running configuration differs from the statup configuration.
```

SUB-TREE

- show snmpv3 view *VIEW-NAME SUB-TREE*

```
Set the OID of the tree.
```

supplicant

- show port-access supplicant

```
Usage: show port-access supplicant [statistics]

Description: Show 802.1X (Port Based Network Access) supplicant
             current status and configuration.
```

Next Available Options:

- -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 449)**
- **statistics** -- Show authentication sessions statistics for 802.1X supplicant.**(p. 510)**

svlans

- show svlans

```
Usage: show vlans [VLAN-ID|ports [ethernet] PORT-LIST]

Description: Show status information for all VLANs.
             If a 'VLAN-ID' is specified, shows the ports that are currently
             members of the VLAN identified by the 'VLAN-ID'.
             If a 'PORT-LIST' is specified, shows all the VLANs of which
             at least one port in the 'PORT-LIST' is a member.
```

Next Available Options:

- **vlan** -- Show detailed VLAN information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**
- **ports** -- Show VLANs that have at least one port from the 'PORT-LIST' as a member. ([ethernet] PORT-LIST) **(p. 498)**

system

- show system

```
Usage: show system [information|power-supplies|temperature|fans]
Description: Show global configured and operational system paramaters
(default is information).
```

Next Available Options:

- **information** -- Show global configured and operational system parameters**(p. 477)**
- **temperature** -- Show systems temperatures and settings**(p. 514)**
- **power-supply** -- Show Chassis Power Supply info and settings**(p. 499)**
- **fans** -- Show system fan status**(p. 471)**

tacacs

- show tacacs

```
Usage: show tacacs

Description: Show TACACS status and statistics.
```

targetaddress

- show snmpv3 targetaddress

```
Show SNMPv3 Target Address table.
```

Next Available Option:

- **TARGETADDR-NAME** -- Show a specifc target address entry. (ASCII-STR) **(p. 513)**

TARGETADDR-NAME

- show snmpv3 targetaddress *TARGETADDR-NAME*

```
Show a specifc target address entry.
```

tcp-udp-port-priority

- show qos tcp-udp-port-priority

```
Usage: show qos tcp-udp-port-priority

Description: Show TCP/UDP port priorities.
```

tech

- show tech

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

Next Available Options:

- **all** -- Display output of a predefined command sequence used by technical support**(p. 453)**
- **buffers** -- Display output of a predefined command sequence used by technical support**(p. 459)**
- **instrumentation** -- Display output of a predefined command sequence used by technical support**(p. 478)**
- **mesh** -- Display output of a predefined command sequence used by technical support**(p. 488)**
- **route** -- Display output of a predefined command sequence used by technical support**(p. 504)**
- **statistics** -- Display output of a predefined command sequence used by technical support**(p. 510)**
- **transceivers** -- Display output of a predefined command sequence used by technical support**(p. 514)**

telnet

- show telnet

```
Usage: show telnet

Description: Show active incoming and outgoing sessions.
```

temperature

- show system temperature

```
Usage: show system temperature

Description: Show systems temperatures and settings.
```

terminal

- show terminal

```
Usage: show terminal

Description: Show logical window dimensions.
```

throttled-hosts

- show connection-rate-filter throttled-hosts

```
Show throttled IP addresses.
```

time

- show cpu *< 1 to 300 >*

```
Time (seconds) over which to average CPU utilization.
```

  Range: < 1 to 300 >

- show time

```
Usage: show time

Description: Show current date and time.
```

timep

- show timep

```
Usage: show timep

Description: Show configured time protocol and servers.
```

transceivers

- show tech transceivers

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

traps

- show ip ospf traps

```
Usage: show ip ospf traps

Description: Show OSPF traps enabled on the device.
```

- show snmp-server traps

```
Show all configured traps.
```

- show spanning-tree traps

```
Show spanning tree trap information.
```

trunks

- show trunks

```
Usage: show trunks [[ethernet] PORT-LIST]

Description: Show a list of ports and the trunks to which they belong.
             If a PORT-LIST is supplied the command shows only the ports
             specified.
```

Next Available Option:

- **port-list** -- Show the trunk information only for the ports specified. ([ethernet] PORT-LIST) **(p. 496)**

type

- show ip ospf link-state type *< router | network | summary | ... >*

```
Show LSAs of the specified type only.
```

Supported Values:

- **router** -- Show router links only.
- **network** -- Show network links only.
- **summary** -- Show summary links only.
- **as-summary** -- Show Autonomous System summary links only.
- **external** -- Show Autonomous System external links only.
- **multicast** -- Show multicast links only.
- **nssa** -- Show NSSA external links only.

- show ip route *< static | connected | rip | ... >*

```
Specify type of routes to display.
```

Supported Values:

- **static** -- Show static routes only.
- **connected** -- Show the switch's interface routes only.
- **rip** -- Show RIP routes only.
- **ospf** -- Show OSPF routes only.

- show ipv6 route *< connected >*

```
Specify type of routes to display.
```

Supported Values:

- **connected** -- Show the switch's interface routes only.

type-of-service

- show qos type-of-service

```
Usage: show qos type-of-service

Description: Show QoS priorities based on IP Type-of-Service.
```

uninstalled

- show licenses uninstalled

```
Display verification key for features which have been uninstalled.
```

uplinks

- show wireless-services *SLOT-ID* uplinks

```
Display uplink ports associated with a wireless-services module.
```

uptime

- show uptime

```
Usage: show uptime

Description: Displays elapsed time since last boot.
```

user

- show snmpv3 group < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | ... > user *USER*

```
Show a specific user.
```

Next Available Option:

- **sec-model** < ver1 | ver2c | ver3 > -- Show a specific security model. **(p. 506)**

- show snmpv3 user

```
Show SNMPv3 users.
```

Next Available Option:

- **USER-NAME** -- Show a specific user. (ASCII-STR) **(p. 516)**

USER-NAME

- show snmpv3 user *USER-NAME*

```
Show a specific user.
```

ver1-2c

- show snmpv3 access-rights < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | ... > sec-model < *ver1* | *ver2c* >

```
Configure SNMPv3 User entry.
```

Supported Values:

- **ver1** -- SNMP version 1 security model.
- **ver2c** -- SNMP version 2c security model.

ver3

- show snmpv3 access-rights < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | ... > sec-model ver3

```
SNMP version 3 security model.
```

Next Available Option:

- **ver3** < noauth | auth | priv > -- Set security level. **(p. 517)**

- show snmpv3 access-rights < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | ... > sec-model ver3 < *noauth* | *auth* | *priv* >

```
Set security level.
```

Supported Values:

- **noauth** -- no authentication (and no privacy)
- **auth** -- authentication (no privacy)
- **priv** -- authentication and privacy

version

- show version

```
Usage: show version

Description: Show software version.
```

view

- show snmpv3 view

```
Show views.
```

Next Available Option:

- **VIEW-NAME** -- Set view name. (ASCII-STR) **(p. 517)**

- show stack view

```
Show the list of devices that are stack members.
```

VIEW-NAME

- show snmpv3 view *VIEW-NAME*

```
Set view name.
```

Next Available Option:

- **SUB-TREE** -- Set the OID of the tree. (ASCII-STR) **(p. 512)**

virtual-link

- show ip ospf virtual-link

```
Usage: show ip ospf virtual-link [IP-ADDR] [area OSPF-AREA-ID]

Description: Show status of all OSPF virtual links configured.
             The 'IP-ADDR' can be specified to display detailed
             information for a particular virtual neighbor. If
             the area is specified only virtual links of the
             area are shown.
```

Next Available Options:

- **vlink-ip** -- Router ID of the link destination for which to show detailed information. (IP-ADDR) **(p. 521)**
- **area** -- Specify area of the virtual links to show. (OSPF-AREA-ID) **(p. 453)**

virtual-neighbor

- show ip ospf virtual-neighbor

```
Usage: show ip ospf virtual-neighbor [IP-ADDR]
                                     [area OSPF-AREA-ID]

Description: Show all virtual neighbors of the device.
             The 'IP-ADDR' can be specified to display detailed
             information for a particular virtual neighbor. If
             the area is specified only virtual neighbors belonging
             to the area are shown.
```

Next Available Options:

- **vneighbor-ip** -- Router ID of the virtual neighbor for which to show detailed information. (IP-ADDR) **(p. 521)**
- **area** -- Specify area of the virtual neighbors to show. (OSPF-AREA-ID) **(p. 453)**

vlan

- show access-list vlan *VLAN-ID*

```
Show ACLs applied to the specified VLAN.
```

- show arp vlan *VLAN-ID*

```
Specify VLAN for which to show ARP entries.
```

- show ip helper-address vlan *VLAN-ID*

```
Specify a vlan for which to show server addresses.
```

- show ip forward-protocol vlan *VLAN-ID*

```
Specify a vlan for which to show server addresses.
```

- show ip igmp *VLAN-ID*

```
Show IGMP operational information for the VLAN specified.
```

Next Available Option:

- **config** -- Show IGMP configuration information for the VLAN specified.**(p. 462)**

- show ip ospf interface vlan *VLAN-ID*

```
Specify VLAN of the interface for which to show detailed information.
```

- show ip rip interface vlan *VLAN-ID*

```
Specify VLAN of the interface for which to show detailed information.
```

- show ipv6 vlan

```
Usage: show ipv6 vlan [VLAN-ID]

Description: Show IPv6 status information for all VLANs.
             If a 'VLAN-ID' is specified, shows the ports that are currently
             members of the VLAN identified by the 'VLAN-ID'.
```

Next Available Option:

- **vlan** -- Show IPv6 information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**

- show ipv6 vlan *VLAN-ID*

```
Show IPv6 information for the VLAN with the ID supplied.
```

- show ipv6 routers vlan

```
Show the IPv6 Router Table Entries for VLAN.
```

Next Available Option:

- **vlan** -- Show IPv6 information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**

- show ipv6 routers vlan *VLAN-ID*

```
Show IPv6 information for the VLAN with the ID supplied.
```

- show ipv6 mld vlan

```
Show MLD VLAN information.
```

Next Available Option:

- **vlan-id** -- Show MLD operational information for the VLAN specified. (VLAN-ID) **(p. 520)**

- show ipv6 neighbors vlan

```
Displays information on the IPv6 neighbor discovery cache
```

Next Available Option:

- **vlan** -- Show IPv6 information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**

- show ipv6 neighbors vlan *VLAN-ID*

```
Show IPv6 information for the VLAN with the ID supplied.
```

- show mac-address vlan *VLAN-ID*

```
Show MAC addresses learned on the specified VLAN.
```

- show port-access authenticator *[ETHERNET] PORT-LIST* vlan

  ```
  Show authorized and unauthorized vlans for 802.1X authenticator.
  ```

- show port-access authenticator vlan

  ```
  Show authorized and unauthorized vlans for 802.1X authenticator.
  ```

- show port-access *[ETHERNET] PORT-LIST* authenticator vlan

  ```
  Show authorized and unauthorized vlans for 802.1X authenticator.
  ```

- show vlans *VLAN-ID*

  ```
  Show detailed VLAN information for the VLAN with the ID supplied.
  ```

- show svlans *VLAN-ID*

  ```
  Show detailed VLAN information for the VLAN with the ID supplied.
  ```

- show vrrp vlan

  ```
  Show VRRP information for a VLAN.
  ```

  Next Available Option:
  - **VLAN-ID** -- Specify VLAN for which to display VRRP information. (VLAN-ID) **(p. 520)**

vlan-id

- show ipv6 mld vlan *VLAN-ID*

  ```
  Show MLD operational information for the VLAN specified.
  ```

  Next Available Options:
  - **config** -- Show MLD configuration information for the VLAN specified.**(p. 462)**
  - **group** -- Show MLD VLAN group info.**(p. 473)**
  - **statistics** -- Show MLD VLAN statistics**(p. 510)**
  - **counters** -- Show MLD VLAN counter information.**(p. 465)**

VLAN-ID

- show ip mroute interface *VLAN-ID*

  ```
  Specify the VLAN ID of the IP multicast routing interface to show.
  ```

- show ip pim interface *VLAN-ID*

  ```
  Specify the VLAN ID of the PIM interface to show.
  ```

- show vrrp vlan *VLAN-ID*

  ```
  Specify VLAN for which to display VRRP information.
  ```

  Next Available Options:
  - **config** -- Show VRRP configuration information for the VLAN. **(p. 462)**
  - **statistics** -- Show VRRP statistics information for the VLAN. **(p. 510)**
  - **vrid** -- Show information for a virtual router. **(p. 521)**

vlan-priority

- show qos vlan-priority

  ```
  Usage: show qos vlan-priority

  Description: Show the VLAN-based priority table.
  ```

vlans

- show wireless-services vlans

  ```
  Display all radio-port VLANs.
  ```

- show igmp-proxy vlans

  ```
  Show all the VLANs currently associated with IGMP proxy domains.
  ```

- show vlans

  ```
  Usage: show vlans [VLAN-ID|ports [ethernet] PORT-LIST]

  Description: Show status information for all VLANs.
               If a 'VLAN-ID' is specified, shows the ports that are currently
               members of the VLAN identified by the 'VLAN-ID'.
               If a 'PORT-LIST' is specified, shows all the VLANs of which
               at least one port in the 'PORT-LIST' is a member.
  ```

  Next Available Options:
  - **vlan** -- Show detailed VLAN information for the VLAN with the ID supplied. (VLAN-ID) **(p. 518)**
  - **ports** -- Show VLANs that have at least one port from the 'PORT-LIST' as a member. ([ethernet] PORT-LIST) **(p. 498)**

vlink-ip

- show ip ospf virtual-link *IP-ADDR*

  ```
  Router ID of the link destination for which to show detailed information.
  ```

vneighbor-ip

- show ip ospf virtual-neighbor *IP-ADDR*

  ```
  Router ID of the virtual neighbor for which to show detailed information.
  ```

vrid

- show vrrp vlan *VLAN-ID* vrid

  ```
  Show information for a virtual router.
  ```

  Next Available Option:
  - **VRID** < 1 to 255 > -- Specify virtual router for which to display information. **(p. 522)**

VRID

- show vrrp vlan *VLAN-ID* vrid *< 1 to 255 >*

  ```
  Specify virtual router for which to display information.
  ```

  Range: < 1 to 255 >

  Next Available Options:

  - **config** -- Show virtual router configuration information. **(p. 462)**
  - **statistics** -- Show virtual router statistics information. **(p. 510)**

vrrp

- show vrrp

  ```
  Usage: show vrrp [...]

  Description: Show VRRP configuration and statistics information.
  ```

  Next Available Options:

  - **config** -- Show VRRP configuration information for the device**(p. 462)**
  - **statistics** -- Show VRRP statistics information for the device**(p. 510)**
  - **vlan** -- Show VRRP information for a VLAN. **(p. 518)**

web-based

- show port-access web-based

  ```
  Usage: show port-access [PORT-LIST] web-based
                          [<config [auth-server|web-server|detail]>|clients]
         show port-access web-based [PORT-LIST]
                          [<config [auth-server|web-server|detail]>|clients]
         show port-access web-based config [PORT-LIST]
                                   [auth-server|web-server|detail]

  Description: Show Web Authentication statistics and configuration. If
               PORT-LIST parameter has been specified then information only
               for the specified ports is shown.
               If 'config' keyword has been specified then the configuration
               of Web Authentication is shown.
               If 'auth-server' keyword has been specified then the
               authentication server-related configuration items are shown.
               If 'web-server' keyword has been specified then the web
               server-related configuration items are shown.
               If PORT-LIST and 'detail' keyword has been specified then the
               detailed configuration of Web Authentication for the specified
               ports is shown.
               If 'clients' keyword has been specified then the current client
               session statistics is shown.
  ```

  Next Available Options:

  - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 449)**
  - **config** -- Show the current configuration of Web Authentication.**(p. 462)**
  - **clients** -- Show the current web client session statistics.**(p. 460)**

- show port-access *[ETHERNET] PORT-LIST* web-based

```
Usage: show port-access [PORT-LIST] web-based
                        [<config [auth-server|web-server|detail]>|clients]
       show port-access web-based [PORT-LIST]
                        [<config [auth-server|web-server|detail]>|clients]
       show port-access web-based config [PORT-LIST]
                                 [auth-server|web-server|detail]

Description: Show Web Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
             of Web Authentication is shown.
             If 'auth-server' keyword has been specified then the
             authentication server-related configuration items are shown.
             If 'web-server' keyword has been specified then the web
             server-related configuration items are shown.
             If PORT-LIST and 'detail' keyword has been specified then the
             detailed configuration of Web Authentication for the specified
             ports is shown.
             If 'clients' keyword has been specified then the current client
             session statistics is shown.
```

Next Available Options:

- **config** -- Show the current configuration of Web Authentication.**(p. 462)**
- **clients** -- Show the current web client session statistics.**(p. 460)**

web-server

- show port-access web-based *[ETHERNET] PORT-LIST* config web-server

```
Show the web server-related configuration items.
```

- show port-access web-based config *[ETHERNET] PORT-LIST* web-server

```
Show the web server-related configuration items.
```

- show port-access web-based config web-server

```
Show the web server-related configuration items.
```

- show port-access *[ETHERNET] PORT-LIST* web-based config web-server

```
Show the web server-related configuration items.
```

wireless-services

- show wireless-services

```
Usage: show wireless-services vlans
       show wireless-services <SLOT-ID>
       show wireless-services <SLOT-ID> [radio-ports|uplinks]

Description: Show wireless-services information.

Parameters:
    o vlans - Display all radio-port VLANs.
    o <SLOT-ID> - Display summary table for the specified slot.
    o <SLOT-ID> radio-ports - Display radio-ports associated with the
                              specified slot.
    o <SLOT-ID> uplinks - Display uplink-ports associated with the
                          specified slot.
```

Next Available Options:

- **vlans** -- Display all radio-port VLANs.**(p. 521)**
- **wireless-services** -- Show wireless-services information (SLOT-ID) **(p. 523)**

- show wireless-services *SLOT-ID*

```
Usage: show wireless-services vlans
       show wireless-services <SLOT-ID>
       show wireless-services <SLOT-ID> [radio-ports|uplinks]

Description: Show wireless-services information.

Parameters:

    o vlans - Display all radio-port VLANs.
    o <SLOT-ID> - Display summary table for the specified slot.
    o <SLOT-ID> radio-ports - Display radio-ports associated with the
                              specified slot.
    o <SLOT-ID> uplinks - Display uplink-ports associated with the
                          specified slot.
```

Next Available Options:

- **radio-ports** -- Display radio-ports associated with a wireless-services module.**(p. 500)**
- **uplinks** -- Display uplink ports associated with a wireless-services module.**(p. 516)**

snmp-server

OVERVIEW

Category:	SNMP
Primary context:	config
Related Commands	**show snmp-server (page 508)**

```
Usage: snmp-server [contact ASCII-STR]
                   [location ASCII-STR]
       [no] snmp-server community ASCII-STR
                   [manager|operator] [restricted|unrestricted]
       [no] snmp-server host IP-ADDR COMMUNITY-STR
                   [none|debug|all|not-info|critical]
       [no] snmp-server enable
       [no] snmp-server enable traps ...
       [no] snmp-server response-source [IP-ADDR|dst-ip-of-request|
                                         loopback<0-7>]
       [no] snmp-server trap-source [IP-ADDR|loopback<0-7>]

Description: Configure the device SNMP server.
   The first version of the command specifies system contact and
   location.

   The second version may be used to add, edit or delete a SNMP community.
   Use 'snmp-server community help' to get a detail of the command.

   The third version defines SNMP traps and their receivers.
   The command configures which network management stations
   will receive SNMP event log messages from the switch and
   the types of events for which the switch will send these
   messages. In all cases, the switch will send all messages
   resulting from thresholds, to the network management
   station that explicitly set each threshold. The levels
   specified on this screen correspond only to the traps set
   for event log messages, not to those set for thresholds.

   You can specify up to 10 trap receivers (network management
   stations).

   The fourth version of the command enables or disables SNMPv1/v2.

   The fifth version Enables/Disables event traps to be sent by the switch.
   Use 'snmp-server enable traps help' to get a detail of the command.

   The sixth version of the command configures the policy for the source-ip
   address of the snmp response pdu. Use 'snmp-server response-source help'
   to get a detail of the command.

   The last version of the command configures the policy for the source-ip
   address of the snmp trap pdu. Use 'snmp-server trap-source help' to get
   a detail of the command.

Parameters:

    o contact ASCII-STR - Up to 48 characters. Name of the switch
```

```
      administrator.

    o location ASCII-STR - Up to 48 characters. Description of the
      switch location.

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.

    o IP-ADDR - Address of the network management station.

    o [none|all|not-info|critical|debug] - The level of Switch
      events that will generate a Trap to be sent: none - send no log
      message; all - send all log messages; not-info - send each log
      message that is not informational-only; critical - send
      critical-level log messages; debug (reserved for Internal use).

    o [IP-ADDR|loopback<0-7>|dst-ip-of-request] - Policy type used to
      fill the source-ip address field of the snmp response/trap pdu:
      IP-ADDR - This ip address will be used while sending the
      snmp response/trap pdu; loopback<0-7> - lexicographically min.
      configured ip address on specified loopback interface will be
      used while sending the response; dst-ip-of-request - destination
      ip address passed in the request pdu will be send as the source-ip
      address in the response pdu.
```

COMMAND STRUCTURE

- [no] snmp-server **community** -- Add/delete SNMP community (ASCII-STR) **(p. 528)**
  - **view < Operator | Manager >** -- Add/delete SNMP community **(p. 534)**
  - **write-access < Restricted | Unrestricted | | ... >** -- Add/delete SNMP community **(p. 534)**
- snmp-server **contact** -- Name of the switch administrator. (ASCII-STR) **(p. 528)**
- [no] snmp-server **enable** -- Enable/Disable SNMPv1/v2 **(p. 529)**
  - **traps** -- Enable/disable event traps to be sent by the switch **(p. 533)**
    - **arp-protect** -- Traps for Dynamic ARP Protection. **(p. 528)**
    - **auth-server-fail** -- Traps reporting authentication server unreachable. **(p. 528)**
    - **dhcp-snooping** -- Traps for DHCP-Snooping. **(p. 529)**
    - **link-change** -- Traps for link-up and link-down. ([ethernet] PORT-LIST) **(p. 531)**
    - **login-failure-mgr** -- Traps for management interface login failure. **(p. 531)**
    - **password-change-mgr** -- Traps for management interface password change. **(p. 532)**
    - **port-security** -- Traps for port access authentication failure. **(p. 532)**
    - **snmp-authentication** -- Select RFC-1157 (standard) or HP-ICF-SNMP (extended) traps. **(p. 533)**
      - **extended** -- Send traps for Extended Authentication failures . **(p. 529)**
      - **standard** -- Send traps for Standard Authentication failures. **(p. 533)**
- [no] snmp-server **host** -- Define SNMP traps and their receivers **(p. 529)**
  - **address** -- IP address of SNMP notification host. (IP-ADDR) **(p. 528)**
  - **address_ipv6** -- IPv6 address of SNMP notification host. (IPV6-ADDR) **(p. 528)**
  - **community** -- Name of the SNMP community (up to 32 characters). (ASCII-STR) **(p. 528)**
  - **events < None | Debug | All | ... >** -- **(p. 529)**

  - **informs** -- Specify if informs will be sent, rather than notifications. **(p. 531)**
    - **retries < 0 to 255 >** -- Specify the number of retries for informs. **(p. 533)**
    - **timeout < 1 to 21474836 >** -- Specify the interval between retries for informs, in seconds. (NUMBER) **(p. 533)**
- snmp-server **location** -- Description of the switch location. (ASCII-STR) **(p. 531)**
- snmp-server **mib** -- Enable/Disable SNMP support for the hpSwitchAuthentication MIB **(p. 532)**
  - **hpSwitchAuthMIB** -- Enable/Disable SNMP support for the hpSwitchAuthentication MIB **(p. 530)**
    - **excluded** -- Disables SNMP support for the hpSwitchAuthentication MIB. **(p. 529)**
    - **included** -- Enables SNMP support for the hpSwitchAuthentication MIB. **(p. 530)**
- [no] snmp-server **response-source** -- Specify the source ip-address policy for the response pdu **(p. 532)**
  - **dst-ip-of-request** -- Destination Ip address of the snmp request pdu will be used as the source ip address in the snmp response pdu. **(p. 529)**
  - **ip-addr** -- IP Address for the source ip address field in the snmp response pdu. (IP-ADDR) **(p. 531)**
  - **loopback < 0 to 7 >** -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the snmp response pdu. **(p. 531)**
- [no] snmp-server **trap-source** -- Specify the source ip-address policy for the trap pdu **(p. 534)**
  - **ip-addr** -- IP Address for the source ip address field in the trap pdu. (IP-ADDR) **(p. 531)**
  - **loopback < 0 to 7 >** -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the trap pdu. **(p. 531)**

EXAMPLES

Example: snmp-server community

Add the following communities:

Community	Access Level	Type of Access
red-team	manager	■ Access to all MIB objects ■ unrestricted (read/write)
blue-team	operator	■ Access to all MIB objects except the CONFIG MIB ■ restricted (read-only)

```
ProCurve(config)# snmp-server community red-team manager unrestricted
ProCurve(config)# snmp-server community blue-team operator restricted
```

COMMAND DETAILS

address

- snmp-server host *IP-ADDR*

```
IP address of SNMP notification host.
```

address_ipv6

- snmp-server host *IPV6-ADDR*

```
IPv6 address of SNMP notification host.
```

arp-protect

- [no] snmp-server enable traps arp-protect

```
Sends a trap if ARP packets are received with an invalid source or destination
MAC address, and invalid IP address, or an invalid IP-to-MAC binding.
```

auth-server-fail

- [no] snmp-server enable traps auth-server-fail

```
Sends a trap if the connection with a RADIUS or TACACS+ authentication server fails.
```

community

- [no] snmp-server community *COMMUNITY*

```
Usage: [no] snmp-server community ASCII-STR
                   [manager|operator] [restricted|unrestricted]

Description: Add/delete SNMP community.

Parameters:

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.
```

Next Available Options:

- **view** < Operator | Manager > -- Add/delete SNMP community**(p. 534)**
- **write-access** < Restricted | Unrestricted | | ... > -- Add/delete SNMP community**(p. 534)**

- snmp-server host *COMMUNITY*

```
Name of the SNMP community (up to 32 characters).
```

contact

- snmp-server contact *CONTACT*

```
Name of the switch administrator.
```

dhcp-snooping

- [no] snmp-server enable traps dhcp-snooping

```
Sends a trap if DHCP packets are received from an untrusted source or if DHCP packets
contain an invalid IP-to_MAC binding.
```

dst-ip-of-request

- snmp-server response-source dst-ip-of-request

```
Destination Ip address of the snmp request pdu will be used as the
source ip address in the snmp response pdu.
```

enable

- [no] snmp-server enable

```
Usage: [no] snmp-server enable

Description:Enable/Disable SNMPv1/v2.
```

Next Available Option:

- **traps** -- Enable/disable event traps to be sent by the switch**(p. 533)**

events

- snmp-server host *< None | Debug | All | ... >*

Supported Values:

- **None** -- Send no log messages.
- **Debug** -- Send debug traps (for Internal use).
- **All** -- Send all log messages
- **Not-INFO** -- Send all but informational-only messages.
- **Critical** -- Send critical-level log messages.

excluded

- snmp-server mib hpSwitchAuthMIB excluded

```
Disables SNMP support for the hpSwitchAuthentication MIB.
```

extended

- [no] snmp-server enable traps snmp-authentication extended

```
Send traps for Extended Authentication failures .
```

host

- [no] snmp-server host

```
Usage: [no] snmp-server host IP-ADDR COMMUNITY-STR
                 [none|debug|all|not-info|critical]
                 [informs [retries RETRY-COUNT] [timeout TIMEOUT]]

Description: Define SNMP traps and their receivers.
             This command configures which network management stations
             will receive SNMP event log messages from the switch and
```

```
                the types of events for which the switch will send these
                messages. In all cases, the switch will send all messages
                resulting from thresholds, to the network management
                station that explicitly set each threshold. The levels
                specified on this screen correspond only to the traps set
                for event log messages, not to those set for thresholds.

                You can specify up to 10 trap receivers (network management
                stations).

Parameters:

    o COMMUNITY-STR - SNMP community string.

    o IP-ADDR - IP address of SNMP notification host.

    o [none|all|not-info|critical|debug] - The level of Switch
      events that will generate a trap to be sent: none - send no log
      message; all - send all log messages; not-info - send each log
      message that is not informational-only; critical - send
      critical-level log messages; debug (reserved for Internal use).

    o [informs [retries RETRY-COUNT] [timeout TIMEOUT]] If 'informs'
      is added to the command, informs rather than traps are sent.
      Retries defines the number of retries to attempt when a response
      is not received. The default is 3. Timeout defines the interval
      between retries, measured in seconds. The default is 15 seconds.
```

Next Available Options:

- **address** -- IP address of SNMP notification host. (IP-ADDR) **(p. 528)**
- **address_ipv6** -- IPv6 address of SNMP notification host. (IPV6-ADDR) **(p. 528)**
- **community** -- Name of the SNMP community (up to 32 characters). (ASCII-STR) **(p. 528)**
- **informs** -- Specify if informs will be sent, rather than notifications.**(p. 531)**
- **events** < None | Debug | All | ... > -- **(p. 529)**

hpSwitchAuthMIB

- snmp-server mib hpSwitchAuthMIB

```
Usage: snmp-server mib hpSwitchAuthMIB <excluded|included>

Description: Enable/Disable SNMP support for the hpSwitchAuthentication MIB.
             When the MIB access is enabled, Manager read/write access
             to the MIB is permitted. Operator read/write access to the MIB
             is always denied. For security reasons, network administrators
             are encouraged to disable SNMPV2c before using the MIB.
```

Next Available Options:

- **included** -- Enables SNMP support for the hpSwitchAuthentication MIB.**(p. 530)**
- **excluded** -- Disables SNMP support for the hpSwitchAuthentication MIB.**(p. 529)**

included

- snmp-server mib hpSwitchAuthMIB included

```
Enables SNMP support for the hpSwitchAuthentication MIB.
```

informs

- snmp-server host informs

```
Specify if informs will be sent, rather than notifications. When an SNMP
Manager receives an inform request, it can send an SNMP response back to the
sending agent. This lets the agent know that the inform request reached its
destination.
```

Next Available Options:

- **retries** < 0 to 255 > -- Specify the number of retries for informs.**(p. 533)**
- **timeout** < 1 to 21474836 > -- Specify the interval between retries for informs, in seconds. (NUMBER) **(p. 533)**

ip-addr

- snmp-server response-source *IP-ADDR*

```
IP Address for the source ip address field in the snmp response pdu.
```

- snmp-server trap-source *IP-ADDR*

```
IP Address for the source ip address field in the trap pdu.
```

link-change

- [no] snmp-server enable traps link-change *[ETHERNET] PORT-LIST*

```
Traps for link-up and link-down.
```

location

- snmp-server location *LOCATION*

```
Description of the switch location.
```

login-failure-mgr

- [no] snmp-server enable traps login-failure-mgr

```
Sends a trap for a failed login with a manager password.
```

loopback

- snmp-server response-source loopback *< 0 to 7 >*

```
For the specified loopback interface, lexicographically minimum
configured ip address will be used as the source ip address in
the snmp response pdu.
```

Range: < 0 to 7 >

- snmp-server trap-source loopback *< 0 to 7 >*

```
For the specified loopback interface, lexicographically minimum
configured ip address will be used as the source ip address in
the trap pdu.
```

Range: < 0 to 7 >

mib

- snmp-server mib

```
Usage: snmp-server mib hpSwitchAuthMIB <excluded|included>

Description: Enable/Disable SNMP support for the hpSwitchAuthentication MIB.
             When the MIB access is enabled, Manager read/write access
             to the MIB is permitted. Operator read/write access to the MIB
             is always denied. For security reasons, network administrators
             are encouraged to disable SNMPV2c before using the MIB.
```

Next Available Option:

- **hpSwitchAuthMIB** -- Enable/Disable SNMP support for the hpSwitchAuthentication MIB**(p. 530)**

password-change-mgr

- [no] snmp-server enable traps password-change-mgr

```
Sends a trap when a manager password is reset.
```

port-security

- [no] snmp-server enable traps port-security

```
Sends a trap for a failed authentication attempt through a web, MAC, or 802.1X
authentication session.
```

response-source

- [no] snmp-server response-source

```
Usage: [no] snmp-server response-source [IP-ADDR|dst-ip-of-request|
                                         loopback<0-7>]

Description: Specify the source ip-address policy for the response pdu.
             By default snmp response pdu will contain the ip address of
             the active interface on which response will be sent. The default
             behavior is in compliance to rfc-1517.
             The no form of the command will revert to default behavior.

IP-ADDR            -- ip-address specified will be used as the source ip
                      address in the snmp response pdu.
dst-ip-of-request  -- Destination ip of the snmp request will be used as
                      the source ip address in the snmp response pdu.
loopback 0-7       -- lexicographically minimum configured ip address on the
                      specified interface will be used as the source ip
                      address in the snmp response pdu.
```

Next Available Options:

- **ip-addr** -- IP Address for the source ip address field in the snmp response pdu. (IP-ADDR) **(p. 531)**
- **dst-ip-of-request** -- Destination Ip address of the snmp request pdu will be used as the source ip address in the snmp response pdu.**(p. 529)**
- **loopback** < 0 to 7 > -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the snmp response pdu.**(p. 531)**

retries

- snmp-server host informs retries *< 0 to 255 >*

```
Maximum number of times to resend an inform request. Default: 3.
```

Range: < 0 to 255 >

snmp-authentication

- [no] snmp-server enable traps snmp-authentication

```
Select RFC-1157 (standard) or HP-ICF-SNMP (extended) traps. Sends a trap for a failed
authentication attempt via SNMP.
```

Next Available Options:

- **standard** -- Send traps for Standard Authentication failures.**(p. 533)**
- **extended** -- Send traps for Extended Authentication failures .**(p. 529)**

standard

- [no] snmp-server enable traps snmp-authentication standard

```
Send traps for Standard Authentication failures.
```

timeout

- snmp-server host informs timeout *< 1 to 21474836 >*

```
Number of seconds to wait for an acknowledgement before resending the
inform request. Default: 15 seconds
```

Range: < 1 to 21474836 >

Default: 15 seconds

traps

- [no] snmp-server enable traps

```
Usage: [no] snmp-server enable traps snmp-authentication <standard | extended>
       [no] snmp-server enable traps port-security
       [no] snmp-server enable traps login-failure-mgr
       [no] snmp-server enable traps password-change-mgr
       [no] snmp-server enable traps authorization
       [no] snmp-server enable traps arp-protect
       [no] snmp-server enable traps dhcp-snooping
       [no] snmp-server enable traps link-change <PORT-LIST>

Description: Enable/disable event traps to be sent
             by the switch.
```

Next Available Options:

- **link-change** -- Traps for link-up and link-down. ([ethernet] PORT-LIST) **(p. 531)**
- **snmp-authentication** -- Select RFC-1157 (standard) or HP-ICF-SNMP (extended) traps.**(p. 533)**
- **dhcp-snooping** -- Traps for DHCP-Snooping.**(p. 529)**
- **arp-protect** -- Traps for Dynamic ARP Protection.**(p. 528)**
- **auth-server-fail** -- Traps reporting authentication server unreachable.**(p. 528)**

- **password-change-mgr** -- Traps for management interface password change.**(p. 532)**
- **login-failure-mgr** -- Traps for management interface login failure.**(p. 531)**
- **port-security** -- Traps for port access authentication failure.**(p. 532)**

trap-source

- [no] snmp-server trap-source

```
Usage: [no] snmp-server trap-source [IP-ADDR|loopback<0-7>]

Description: Specify the source ip-address policy for the trap pdu.
             By default snmp trap pdu will contain the ip address of
             the active interface on which trap will be sent. The default
             behavior is in compliance to rfc-1517.
             The no form of the command will revert to default behavior.

IP-ADDR            -- ip-address specified will be used as the source ip
                      address in the generated trap.
loopback 0-7       -- lexicographically minimum configured ip address on the
                      specified interface will be used as the source ip
                      address in the generated trap pdu.
```

Next Available Options:

- **ip-addr** -- IP Address for the source ip address field in the trap pdu. (IP-ADDR) **(p. 531)**
- **loopback** < 0 to 7 > -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the trap pdu.**(p. 531)**

view

- [no] snmp-server community *COMMUNITY* *< Operator | Manager >*

```
Usage: [no] snmp-server community ASCII-STR
                  [manager|operator] [restricted|unrestricted]

Description: Add/delete SNMP community.

Parameters:

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.
```

Supported Values:

- **Operator** -- The community can access all except the CONFIG MIB.
- **Manager** -- The community can access all MIB objects.

write-access

- [no] snmp-server community *COMMUNITY* *< Restricted | Unrestricted | | ... >*

```
Usage: [no] snmp-server community ASCII-STR
                   [manager|operator] [restricted|unrestricted]

Description: Add/delete SNMP community.

Parameters:

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.
```

Supported Values:

- **Restricted** -- MIB variables cannot be set, only read.
- **Unrestricted** -- Any MIB variable that has read/write access can be set.
-
- **Unrestricted**

snmpv3

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show snmpv3 (page 508)** **show snmp-server (page 508)**

```
Usage: [no] snmpv3 <community|group|notify|params|restricted-access|
                    targetaddress|user>

Description: Configure SNMPv3 features.
```

NOTES

IPv6 Supported Commands

IPv6 addressing is supported for the following commands:

- snmpv3 targetaddress <name> params <params-name>

  for

  - addr-mask <ip-addr>
  - filter <none | debug | all | not-info | critical>
  - max-msg-size <484 - 65535>
  - port-mask <tcp-udp port>
  - retries <0-255>
  - taglist <tag-name>
  - timeout <0 - 2147483647>
  - udp-port-number <port-number>

COMMAND STRUCTURE

- [no] snmpv3 **community** -- Configure SNMPv3 Community entry. **(p. 539)**
  - **index** -- Set community index. (ASCII-STR) **(p. 540)**
    - **name** -- Set community name. (ASCII-STR) **(p. 541)**
      - **sec-name** -- Set security name. (ASCII-STR) **(p. 544)**
        - **tag** -- Set tag value for the community (ASCII-STR) **(p. 544)**
- [no] snmpv3 **enable** -- Enable SNMPv3. **(p. 539)**
- [no] snmpv3 **engineid** -- Configure SNMPv3 engineID. (ASCII-STR) **(p. 539)**
- [no] snmpv3 **group** **< ManagerPriv | ManagerAuth | OperatorAuth | ... >** -- Configure SNMPv3 User to Group entry. **(p. 540)**
  - **user** -- Set user to be added to the group. (ASCII-STR) **(p. 545)**
    - **sec-model** **< ver1 | ver2c | ver3 >** -- Set security model to be used. **(p. 544)**
- [no] snmpv3 **notify** -- Configure SNMPv3 Notification entry. (ASCII-STR) **(p. 541)**

    - **tagvalue** -- Set tag value that selects entries in the snmpTargetAddr table. (ASCII-STR) **(p. 545)**
- [no] snmpv3 **only** -- Accept only SNMP v3 messages. **(p. 542)**
- [no] snmpv3 **params** -- Configure SNMPv3 Target Parameter entry. (ASCII-STR) **(p. 542)**
    - **user** -- Set user that the switch will send messages on behalf. (ASCII-STR) **(p. 545)**
        - **sec-model** -- Set security model. **(p. 544)**
            - **sec-model12c < ver1 | ver2c >** -- Configure SNMPv3 User entry. **(p. 544)**
                - **message-processing < ver1 | ver2c | ver3 >** -- Set message processing model value. **(p. 541)**
            - **ver3** -- SNMP version 3 security model. **(p. 546)**
                - **message-processing** -- Set message processing model value. **(p. 541)**
                    - **ver3 < noauth | auth | priv >** -- Set security level. **(p. 546)**
- [no] snmpv3 **restricted-access** -- Configure SNMPv1 and SNMPv2c access properties. **(p. 543)**
- [no] snmpv3 **targetaddress** -- Configure SNMPv3 Target Address entry. (ASCII-STR) **(p. 545)**
    - **params** -- Set parameter name. (ASCII-STR) **(p. 542)**
        - **ipaddr** -- Set IP address of the destination target. (IP-ADDR) **(p. 540)**
            - **addr-mask** -- Set range of transport addresses with this mask. (IP-ADDR) **(p. 538)**
            - **filter < None | Debug | All | ... >** -- Set log filters. **(p. 539)**
            - **max-msg-size < 484 to 65535 >** -- Set maximum message size value; default is 1472. **(p. 541)**
            - **port-mask** -- Set range of udp ports with this mask. (TCP/UDP-PORT) **(p. 542)**
            - **retries < 0 to 255 >** -- Set retries value; default is 3. **(p. 543)**
            - **taglist** -- Set list of values used to select this entry from snmpNotifyTable. (ASCII-STR) **(p. 544)**
            - **timeout < 0 to 2147483647 >** -- Set time-out value; default is 1500. **(p. 545)**
            - **udp-port** -- Set UDP port number to which the messages are sent; default is 162. (TCP/UDP-PORT) **(p. 545)**
        - **ipv6addr** -- Set IPv6 address of the destination target. (IPV6-ADDR) **(p. 540)**
            - **addr-mask** -- Set range of transport addresses with this mask. (IP-ADDR) **(p. 538)**
            - **filter < None | Debug | All | ... >** -- Set log filters. **(p. 539)**
            - **max-msg-size < 484 to 65535 >** -- Set maximum message size value; default is 1472. **(p. 541)**
            - **port-mask** -- Set range of udp ports with this mask. (TCP/UDP-PORT) **(p. 542)**
            - **retries < 0 to 255 >** -- Set retries value; default is 3. **(p. 543)**
            - **taglist** -- Set list of values used to select this entry from snmpNotifyTable. (ASCII-STR) **(p. 544)**
            - **timeout < 0 to 2147483647 >** -- Set time-out value; default is 1500. **(p. 545)**
            - **udp-port** -- Set UDP port number to which the messages are sent; default is 162. (TCP/UDP-PORT) **(p. 545)**
- [no] snmpv3 **user** -- Configure SNMPv3 User entry. **(p. 545)**
    - **username** -- Set authentication paramaters. (ASCII-STR) **(p. 546)**
        - **auth** -- Set authentication paramaters. **(p. 538)**
            - **authpassword** -- Set authentication password. (ASCII-STR) **(p. 538)**
                - **priv** -- Set Privacy password. **(p. 542)**
                    - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**
                    - **privprotocol < DES | AES >** -- Set privacy protocol. **(p. 543)**
                        - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**
            - **authprotocol < MD5 | SHA >** -- Set authentication protocol. **(p. 538)**
                - **authpassword** -- Set authentication password. (ASCII-STR) **(p. 538)**
                    - **priv** -- Set Privacy password. **(p. 542)**
                        - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**
                        - **privprotocol < DES | AES >** -- Set privacy protocol. **(p. 543)**
                            - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**

COMMAND DETAILS

addr-mask

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* addr-mask *IP-ADDR*

```
Set range of transport addresses with this mask.
```

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* addr-mask *IP-ADDR*

```
Set range of transport addresses with this mask.
```

auth

- snmpv3 user *USERNAME* auth

```
Set authentication paramaters.
```

Next Available Options:

- **authpassword** -- Set authentication password. (ASCII-STR) **(p. 538)**
- **authprotocol** < MD5 | SHA > -- Set authentication protocol. **(p. 538)**

authpassword

- snmpv3 user *USERNAME* auth *AUTHPASSWORD*

```
Set authentication password.
```

Next Available Option:

- **priv** -- Set Privacy password. **(p. 542)**

- snmpv3 user *USERNAME* auth *< MD5 | SHA > AUTHPASSWORD*

```
Set authentication password.
```

Next Available Option:

- **priv** -- Set Privacy password. **(p. 542)**

authprotocol

- snmpv3 user *USERNAME* auth *< MD5 | SHA >*

```
Set authentication protocol.
```

Supported Values:

- **MD5** -- Set the authentication protocol to md5.
- **SHA** -- Set the authentication protocol to sha.

Next Available Option:

- **authpassword** -- Set authentication password. (ASCII-STR) **(p. 538)**

community

- [no] snmpv3 community

  ```
  Configure SNMPv3 Community entry.
  ```

  Next Available Option:

  - **index** -- Set community index. (ASCII-STR) **(p. 540)**

enable

- [no] snmpv3 enable

  ```
  Enable SNMPv3.
  ```

engineid

- [no] snmpv3 engineid *ENGINEID*

  ```
  Configure SNMPv3 engineID.
  ```

filter

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* filter *< None | Debug | All | ... >*

  ```
  Set log filters.
  ```

  Supported Values:

  - **None** -- Send no log messages.
  - **Debug** -- Send debug traps (for Internal use).
  - **All** -- Send all log messages
  - **Not-INFO** -- Send all but informational-only messages.
  - **Critical** -- Send critical-level log messages.
- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* filter *< None | Debug | All | ... >*

  ```
  Set log filters.
  ```

  Supported Values:

  - **None** -- Send no log messages.
  - **Debug** -- Send debug traps (for Internal use).
  - **All** -- Send all log messages
  - **Not-INFO** -- Send all but informational-only messages.
  - **Critical** -- Send critical-level log messages.

group

- [no] snmpv3 group < *ManagerPriv* | *ManagerAuth* | *OperatorAuth* | ... >

```
Configure SNMPv3 User to Group entry.
```

Supported Values:

- **ManagerPriv** -- Require privacy and authentication, can access all objects.
- **ManagerAuth** -- Require authentication, can access all objects.
- **OperatorAuth** -- Requires authentication, limited access to objects.
- **OperatorNoAuth** -- No authentication required, limited access to objects.
- **ComManagerRW** -- Community with manager and unrestricted write access.
- **ComManagerR** -- Community with manager and restricted write access.
- **ComOperatorRW** -- Community with operator and unrestricted write access.
- **ComOperatorR** -- Community with operator and restricted write access.

Next Available Option:

- **user** -- Set user to be added to the group. (ASCII-STR) **(p. 545)**

index

- [no] snmpv3 community index *INDEX*

```
Set community index.
```

Next Available Option:

- **name** -- Set community name. (ASCII-STR) **(p. 541)**

ipaddr

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR*

```
Set IP address of the destination target.
```

Next Available Options:

- **addr-mask** -- Set range of transport addresses with this mask. (IP-ADDR) **(p. 538)**
- **filter** < None | Debug | All | ... > -- Set log filters. **(p. 539)**
- **max-msg-size** < 484 to 65535 > -- Set maximum message size value; default is 1472. **(p. 541)**
- **port-mask** -- Set range of udp ports with this mask. (TCP/UDP-PORT) **(p. 542)**
- **retries** < 0 to 255 > -- Set retries value; default is 3. **(p. 543)**
- **timeout** < 0 to 2147483647 > -- Set time-out value; default is 1500. **(p. 545)**
- **taglist** -- Set list of values used to select this entry from snmpNotifyTable. (ASCII-STR) **(p. 544)**
- **udp-port** -- Set UDP port number to which the messages are sent; default is 162. (TCP/UDP-PORT) **(p. 545)**

ipv6addr

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR*

```
Set IPv6 address of the destination target.
```

Next Available Options:

- **addr-mask** -- Set range of transport addresses with this mask. (IP-ADDR) **(p. 538)**
- **filter** < None | Debug | All | ... > -- Set log filters. **(p. 539)**

- **max-msg-size** < 484 to 65535 > -- Set maximum message size value; default is 1472. **(p. 541)**
- **port-mask** -- Set range of udp ports with this mask. (TCP/UDP-PORT) **(p. 542)**
- **retries** < 0 to 255 > -- Set retries value; default is 3. **(p. 543)**
- **timeout** < 0 to 2147483647 > -- Set time-out value; default is 1500. **(p. 545)**
- **taglist** -- Set list of values used to select this entry from snmpNotifyTable. (ASCII-STR) **(p. 544)**
- **udp-port** -- Set UDP port number to which the messages are sent; default is 162. (TCP/UDP-PORT) **(p. 545)**

max-msg-size

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* max-msg-size *< 484 to 65535 >*

  ```
  Set maximum message size value; default is 1472.
  ```

  Range: < 484 to 65535 >
- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* max-msg-size *< 484 to 65535 >*

  ```
  Set maximum message size value; default is 1472.
  ```

  Range: < 484 to 65535 >

message-processing

- snmpv3 params *PARAMS* user *USER* sec-model *< ver1 | ver2c >* message-processing *< ver1 | ver2c | ver3 >*

  ```
  Set message processing model value.
  ```

  Supported Values:
  - **ver1** -- SNMP version 1 message processing model.
  - **ver2c** -- SNMP version 2c message processing model.
  - **ver3** -- SNMP version 3 message processing model.
- snmpv3 params *PARAMS* user *USER* sec-model ver3 message-processing

  ```
  Set message processing model value.
  ```

  Next Available Option:
  - **ver3** < noauth | auth | priv > -- Set security level. **(p. 546)**

name

- snmpv3 community index *INDEX* name *NAME*

  ```
  Set community name.
  ```

  Next Available Option:
  - **sec-name** -- Set security name. (ASCII-STR) **(p. 544)**

notify

- [no] snmpv3 notify *NOTIFY*

  ```
  Configure SNMPv3 Notification entry.
  ```

Next Available Option:

- **tagvalue** -- Set tag value that selects entries in the snmpTargetAddr table. (ASCII-STR) **(p. 545)**

only

- [no] snmpv3 only

  `Accept only SNMP v3 messages.`

params

- [no] snmpv3 params *PARAMS*

  `Configure SNMPv3 Target Parameter entry.`

  Next Available Option:

  - **user** -- Set user that the switch will send messages on behalf. (ASCII-STR) **(p. 545)**

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS*

  `Set parameter name.`

  Next Available Options:

  - **ipaddr** -- Set IP address of the destination target. (IP-ADDR) **(p. 540)**
  - **ipv6addr** -- Set IPv6 address of the destination target. (IPV6-ADDR) **(p. 540)**

port-mask

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* port-mask *TCP/UDP-PORT*

  `Set range of udp ports with this mask.`

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* port-mask *TCP/UDP-PORT*

  `Set range of udp ports with this mask.`

priv

- snmpv3 user *USERNAME* auth *AUTHPASSWORD* priv

  `Set Privacy password.`

  Next Available Options:

  - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**
  - **privprotocol** < DES | AES > -- Set privacy protocol. **(p. 543)**

- snmpv3 user *USERNAME* auth *< MD5 | SHA > AUTHPASSWORD* priv

  `Set Privacy password.`

  Next Available Options:

  - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**
  - **privprotocol** < DES | AES > -- Set privacy protocol. **(p. 543)**

privpassword

- snmpv3 user *USERNAME* auth *AUTHPASSWORD* priv *PRIVPASSWORD*

  ```
  Set Privacy password.
  ```

- snmpv3 user *USERNAME* auth *AUTHPASSWORD* priv < *DES* | *AES* > *PRIVPASSWORD*

  ```
  Set Privacy password.
  ```

- snmpv3 user *USERNAME* auth < *MD5* | *SHA* > *AUTHPASSWORD* priv *PRIVPASSWORD*

  ```
  Set Privacy password.
  ```

- snmpv3 user *USERNAME* auth < *MD5* | *SHA* > *AUTHPASSWORD* priv < *DES* | *AES* > *PRIVPASSWORD*

  ```
  Set Privacy password.
  ```

privprotocol

- snmpv3 user *USERNAME* auth *AUTHPASSWORD* priv < *DES* | *AES* >

  ```
  Set privacy protocol.
  ```

  Supported Values:
  - **DES** -- Set the privacy protocol to des.
  - **AES** -- Set the privacy protocol to aes-128.

  Next Available Option:
  - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**

- snmpv3 user *USERNAME* auth < *MD5* | *SHA* > *AUTHPASSWORD* priv < *DES* | *AES* >

  ```
  Set privacy protocol.
  ```

  Supported Values:
  - **DES** -- Set the privacy protocol to des.
  - **AES** -- Set the privacy protocol to aes-128.

  Next Available Option:
  - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 543)**

restricted-access

- [no] snmpv3 restricted-access

  ```
  Configure SNMPv1 and SNMPv2c access properties.
  ```

retries

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* retries < *0 to 255* >

  ```
  Set retries value; default is 3.
  ```

  Range: < 0 to 255 >

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* retries *< 0 to 255 >*

  ```
  Set retries value; default is 3.
  ```

  Range: < 0 to 255 >

sec-model

- [no] snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* user *USER* sec-model *< ver1 | ver2c | ver3 >*

  ```
  Set security model to be used.
  ```

  Supported Values:
  - **ver1** -- SNMP version 1 security model.
  - **ver2c** -- SNMP version v2c security model.
  - **ver3** -- SNMP version 3 security model.
- snmpv3 params *PARAMS* user *USER* sec-model

  ```
  Set security model.
  ```

  Next Available Options:
  - **sec-model12c** < ver1 | ver2c > -- Configure SNMPv3 User entry.**(p. 544)**
  - **ver3** -- SNMP version 3 security model.**(p. 546)**

sec-model12c

- snmpv3 params *PARAMS* user *USER* sec-model *< ver1 | ver2c >*

  ```
  Configure SNMPv3 User entry.
  ```

  Supported Values:
  - **ver1** -- SNMP version 1 security model.
  - **ver2c** -- SNMP version 2c security model.

  Next Available Option:
  - **message-processing** < ver1 | ver2c | ver3 > -- Set message processing model value. **(p. 541)**

sec-name

- snmpv3 community index *INDEX* name *NAME* sec-name *SEC-NAME*

  ```
  Set security name.
  ```

  Next Available Option:
  - **tag** -- Set tag value for the community (ASCII-STR) **(p. 544)**

tag

- snmpv3 community index *INDEX* name *NAME* sec-name *SEC-NAME* tag *TAG*

  ```
  Set tag value for the community
  ```

taglist

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* taglist *TAGLIST*

```
Set list of values used to select this entry from snmpNotifyTable.
```

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* taglist *TAGLIST*

```
Set list of values used to select this entry from snmpNotifyTable.
```

tagvalue

- snmpv3 notify *NOTIFY* tagvalue *TAGVALUE*

```
Set tag value that selects entries in the snmpTargetAddr table.
```

targetaddress

- [no] snmpv3 targetaddress *TARGETADDRESS*

```
Configure SNMPv3 Target Address entry.
```

Next Available Option:

- **params** -- Set parameter name. (ASCII-STR) **(p. 542)**

timeout

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* timeout *< 0 to 2147483647 >*

```
Set time-out value; default is 1500.
```

Range: < 0 to 2147483647 >

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* timeout *< 0 to 2147483647 >*

```
Set time-out value; default is 1500.
```

Range: < 0 to 2147483647 >

udp-port

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* udp-port *TCP/UDP-PORT*

```
Set UDP port number to which the messages are sent; default is 162.
```

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IPV6-ADDR* udp-port *TCP/UDP-PORT*

```
Set UDP port number to which the messages are sent; default is 162.
```

user

- [no] snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* user *USER*

```
Set user to be added to the group.
```

Next Available Option:

- **sec-model** < ver1 | ver2c | ver3 > -- Set security model to be used. **(p. 544)**

- snmpv3 params *PARAMS* user *USER*

```
Set user that the switch will send messages on behalf.
```

Next Available Option:

- **sec-model** -- Set security model. **(p. 544)**

- [no] snmpv3 user

  `Configure SNMPv3 User entry.`

  Next Available Option:

  - **username** -- Set authentication paramaters. (ASCII-STR) **(p. 546)**

username

- snmpv3 user *USERNAME*

  `Set authentication paramaters.`

  Next Available Option:

  - **auth** -- Set authentication paramaters. **(p. 538)**

ver3

- snmpv3 params *PARAMS* user *USER* sec-model ver3

  `SNMP version 3 security model.`

  Next Available Option:

  - **message-processing** -- Set message processing model value. **(p. 541)**

- snmpv3 params *PARAMS* user *USER* sec-model ver3 message-processing ver3 *< noauth | auth | priv >*

  `Set security level.`

  Supported Values:

  - **noauth** -- no authentication (and no privacy)
  - **auth** -- authentication (no privacy)
  - **priv** -- authentication and privacy

sntp

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show sntp (page 508)** **timesync (page 597)**

```
Usage: [no] sntp [broadcast|unicast]
       [no] sntp server priority <PRIORITY> <IP-ADDR | IPV6-ADDR> [version]
       sntp poll-interval <30-720>

Description: Configure the Simple Network Time Protocol (SNTP).

             The first version of the command specifies whether the
             switch operates in broadcast or unicast mode. If no mode is
             specified then the mode defaults to broadcast.

             The second version of the command adds or deletes an SNTP
             server to or from the configuration. The maximum number of
             SNTP servers that can be configured is 3. Version can have
             a value between 1 and 7. If no version is specified then a
             default value of 3 is used.Priority specifies the order in
             which the configured servers are polled for getting the time.
             It can have a value between 1 and 3.

             The final version of this command sets the SNTP poll
             interval, which specifies the amount of time between updates
             of the system clock via SNTP.
```

COMMAND STRUCTURE

- sntp **broadcast** -- Operate in broadcast mode **(p. 548)**
- sntp **poll-interval < 30 to 720 >** -- The amount of time between updates of the system clock via SNTP **(p. 548)**
- [no] sntp **server** -- Configure SNTP servers to poll time from. **(p. 548)**
  - **priority < 1 to 3 >** -- Priority of the Server Address. (NUMBER) **(p. 548)**
    - **ipaddr** -- SNTP server IPv4 address. (IP-ADDR) **(p. 548)**
      - **version < 1 to 7 >** -- Version of the SNTP server. **(p. 549)**
    - **ipv6addr** -- SNTP server IPv6 address. (IPV6-ADDR) **(p. 548)**
      - **version < 1 to 7 >** -- Version of the SNTP server. **(p. 549)**
- sntp **unicast** -- Operate in unicast mode **(p. 549)**

EXAMPLES

Example: sntp poll-interval SECONDS

Change the SNTP poll interval to 300 seconds:

```
HPswitch(config)# sntp poll-interval 300
```

COMMAND DETAILS

broadcast (p. 548)	**poll-interval (p. 548)**	**unicast (p. 549)**

broadcast

- sntp broadcast

```
Operate in broadcast mode
```

ipaddr

- [no] sntp server priority *< 1 to 3 > IP-ADDR*

```
SNTP server IPv4 address.
```

Next Available Option:

- **version** < 1 to 7 > -- Version of the SNTP server.**(p. 549)**

ipv6addr

- [no] sntp server priority *< 1 to 3 > IPV6-ADDR*

```
SNTP server IPv6 address.
```

Next Available Option:

- **version** < 1 to 7 > -- Version of the SNTP server.**(p. 549)**

poll-interval

- sntp *< 30 to 720 >*

```
The amount of time between updates of the system clock via SNTP
```

Range: < 30 to 720 >

priority

- sntp server priority *< 1 to 3 >*

```
Specifies the order in which the configured servers are polled for getting the time.
```

Range: < 1 to 3 >

Next Available Options:

- **ipaddr** -- SNTP server IPv4 address. (IP-ADDR) **(p. 548)**
- **ipv6addr** -- SNTP server IPv6 address. (IPV6-ADDR) **(p. 548)**

server

- [no] sntp server

```
Configure SNTP servers to poll time from.
```

Next Available Option:

- **priority** < 1 to 3 > -- Priority of the Server Address. (NUMBER) **(p. 548)**

unicast

- sntp unicast

  ```
  Operate in unicast mode
  ```

version

- sntp server priority *< 1 to 3 > IP-ADDR < 1 to 7 >*

  ```
  Version of the SNTP server.
  ```

  Range: < 1 to 7 >
- sntp server priority *< 1 to 3 > IPV6-ADDR < 1 to 7 >*

  ```
  Version of the SNTP server.
  ```

  Range: < 1 to 7 >

spanning-tree

OVERVIEW

Category:	
Primary context:	config
Related Commands	**show spanning-tree (page 509)**

```
Usage: [no] spanning-tree [[ethernet] PORT-LIST ...]
             [pending ...]
             [instance ...]
             [legacy-mode]
             [legacy-path-cost]
             [config-name ASCII-STR]
             [config-revision <0-65535>]
             [max-hops <1-40>]
             [force-version <stp-compatible|rstp-operation|mstp-operation>]
             [trap <errant-bpdu>]
             [forward-delay <4-30>]
             [hello-time <1-10>]
             [maximum-age <6-40>]
             [bpdu-protection-timeout]
             [priority <<0-15>|<0-65535>>]

Description: Set the parameters for operation of the switch in a spanning tree
             topology.
             Note - the default spanning tree configuration complies with the
             IEEE 802.1s, Multiple Spanning Tree Protocol (MSTP), standard
             recommended values and should not be changed without thorough
             knowledge of spanning tree operation.
             If 'no' is used the command disables the spanning tree operation.
             Parameters are not allowed with 'no' option.

Parameters:

    o ethernet PORT-LIST ... - Configure the port-specific parameters.
      Use 'spanning-tree [ethernet] PORT-LIST ?' to get a list of all
      possible configuration options, or 'spanning-tree [ethernet]
      PORT-LIST help' to get a detailed help for this form of the command.
    o force-version (default: native mode) - Set Spanning Tree protocol
      compatibility mode on the device. Forces current protocol engine to
      emulate behavior of earlier versions of spanning tree protocol or
      operate in the native mode. The value of this parameter applies to
      all ports of the switch.
    o forward-delay <4-30> (default: 15) - Time (in seconds) the switch
      waits between transitioning from listening to learning and from
      learning to forwarding states.
    o hello-time <1-10> (default: 2) - Time (in seconds) between messages
      transmitted when the switch is root. The parameter is in force
      for all switch ports in RSTP and STP modes. If the MSTP engine is
      running this global value can be changed for individual ports.
    o maximum-age <6-40> (default: 20) - Maximum message age (in seconds)
      of received STP information before it is discarded.
    0 bpdu-protection-timeout - The duration of time (in seconds) when a
      protected port affected by receiving of an unauthorized BPDU will
      remain in down state. The zero value means infinity.
```

```
o priority <0-15> or <0-65535> (default is 32768 and step 8 respectively) -
  The device priority - used along with the switch MAC address to determine
  which device is the root. If 802.1w or 802.1s STP version is set, then
  the range of 0-61440 is divided into steps of 4096. These steps are
  numbered from 0 to 15.
o config-name ASCII-STR (default is switch's MAC address) - The name of
  the MST region configuration identifier. The name has the maximum length
  of 32 characters and is case sensitive. Use "no" form of the command
  to reset to the default name. The parameter is configurable in MSTP mode
  only.
o config-revision <0-65535> (default is 0) - The revision number of the MST
  region configuration identifier. The parameter is configurable in MSTP
  mode only.
o max-hops <1-40> (default is 20) - The number of hops in the MST region
  before the MST BPDU is discarded and the information held for a port is
  aged. This parameter is configurable in MSTP mode only and serves for
  the same purpose as the maximum-age and message-age couple used by
  legacy single spanning tree bridges.
o instance ... - Allows to create, delete and configure MST instances.
  This command is available in MSTP mode only. See the command help for
  further details.
o pending ... - Manipulate the pending MSTP configuration. This command
  is available in MSTP mode only. See the command help for more details.
o legacy-path-cost - Set default pathcosts to 802.1D (legacy)  or 802.1t
  (not legacy) values. This command is available in MSTP mode only.
o legacy-mode - Set spanning-tree protocol to operate either in 802.1D
  legacy mode or in 802.1s native mode. This command is available in MSTP
  mode only. See the command help for more details.
o trap - Enable/disable STP traps. The following traps are generated
         as a result of finding an unusual condition on a switch port.
         Possible trap names are:
       - 'errant-bpdu' signifies that an unexpected Spanning Tree BPDU
         has been received on a port.
```

COMMAND STRUCTURE

- spanning-tree **bpdu-protection-timeout** **< 0 to 65535 >** -- Set the time for protected ports to be in down state after receiving unauthorized BPDUs. **(p. 554)**
- spanning-tree **clear-debug-counters** -- Clear spanning tree debug counters. **(p. 554)**
  - **instance** **< 0 to 16 >** -- Clear spanning tree instance debug counters. (NUMBER) **(p. 556)**
    - **ports** -- Clear spanning tree port(s) debug counters. ([ethernet] PORT-LIST) **(p. 564)**
  - **ports** -- Clear spanning tree port(s) debug counters. ([ethernet] PORT-LIST) **(p. 564)**
    - **instance** **< 0 to 16 >** -- Clear spanning tree instance debug counters. (NUMBER) **(p. 556)**
- [no] spanning-tree **config-name** -- Set the MST region configuration name (default is switch's MAC address). **(p. 555)**
  - **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 555)**
- spanning-tree **config-revision** **< 0 to 65535 >** -- Set the MST region configuration revision number (default is 0). **(p. 555)**
- spanning-tree **force-version** **< STP-compatible | RSTP-operation >** -- Set Spanning Tree protocol compatibility mode. **(p. 555)**
- spanning-tree **force-version** **< STP-compatible | RSTP-operation | MSTP-operation >** -- Set Spanning Tree protocol compatibility mode. **(p. 555)**
- spanning-tree **forward-delay** **< 4 to 30 >** -- Set time the switch waits between transitioning from listening to learning and from learning to forwarding states. **(p. 556)**
- spanning-tree **hello-time** **< 1 to 10 >** -- Set time between messages transmission when the switch is root. **(p. 556)**
- [no] spanning-tree **instance** -- Create, delete or configure an MST instance **(p. 556)**

  - **ist** -- Configure internal spanning tree (IST) instance. **(p. 557)**
    - **port-list** -- Configure internal spanning tree (IST) instance ports parameters ([ethernet] PORT-LIST) **(p. 560)**
      - **path-cost** -- Set the internal port pathcost for the IST (default is 'auto'). **(p. 558)**
        - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 554)**
        - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 558)**
  - **MSTID < 1 to 16 >** -- ID of the MST instance to configure. **(p. 558)**
    - **port-list** -- Configure MST instance ports parameters ([ethernet] PORT-LIST) **(p. 560)**
      - **path-cost** -- Set the port pathcost for the instance (default is 'auto'). **(p. 558)**
        - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 554)**
        - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 558)**
      - **priority < 0 to 15 >** -- Set the port priority for the instance (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8). **(p. 564)**
    - **priority < 0 to 15 >** -- Set the device priority for the MST instance (the value is in range of 0-61440 divided into steps of 4096 that are numbered from 0 to 15, default is step 8). **(p. 564)**
    - **vlan** -- Configure VLANs for the MST instance. **(p. 566)**
      - **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 566)**
- [no] spanning-tree **legacy-mode** -- Set spanning-tree protocol to operate either in 802.1D legacy mode or in 802.1s native mode. 'spanning-tree legacy-mode' is the equivalent of executing: spanning-tree legacy-path-cost spanning-tree force-version stp-compatible 'no spanning-tree legacy-mode' is the equivalent of executing: no spanning-tree legacy-path-cost spanning-tree force-version mstp-operation **(p. 557)**
- [no] spanning-tree **legacy-path-cost** -- Set 802.1D (legacy) or 802.1t (not legacy) default pathcost values. **(p. 557)**
- spanning-tree **max-hops < 1 to 40 >** -- Set the max number of hops in a region before the MST BPDU is discarded and the information held for a port is aged (default is 20). **(p. 558)**
- spanning-tree **maximum-age < 6 to 40 >** -- Set maximum age of received STP information before it is discarded. **(p. 558)**
- [no] spanning-tree **pending** -- Manipulate pending MSTP configuration **(p. 560)**
  - **apply** -- Apply pending MSTP configuration (swaps active and pending configuratons). **(p. 553)**
  - **config-name** -- Set the pending MST region configuration name (default is switch's MAC address). **(p. 555)**
    - **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 555)**
  - **config-revision < 0 to 65535 >** -- Set the pending MST region configuration revision number (default is 0). **(p. 555)**
  - **instance** -- Change pending MST instance configuration. **(p. 556)**
    - **MSTID < 1 to 16 >** -- ID of the MST instance to configure. **(p. 558)**
      - **vlan** -- Configure VLANs for the MST instance. **(p. 566)**
        - **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 566)**
  - **reset** -- Copy active configuration to pending. **(p. 565)**
- [no] spanning-tree **port-list** -- Configure the port-specific parameters of the spanning tree protocol for individual ports ([ethernet] PORT-LIST) **(p. 560)**
  - **admin-edge-port** -- Set the administrative edge port status. **(p. 553)**
  - **auto-edge-port** -- Set the automatic edge port detection. **(p. 554)**
  - **bpdu-filter** -- Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a continuous fowarding state. **(p. 554)**
  - **bpdu-protection** -- Disable the specific port or ports if the port(s) receives STP BPDUs. **(p. 554)**
  - **hello-time** -- Set message transmission interval (in sec.) on the port. **(p. 556)**
    - **global** -- Use the globally configured hello-time value. **(p. 556)**
    - **hello-time < 1 to 10 >** -- Set message transmission interval (in sec.) on the port. **(p. 556)**

  - **mcheck** -- Force the port to transmit RST BPDUs. **(p. 558)**
  - **path-cost** -- Set port's path cost value. **(p. 558)**
    - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 554)**
    - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 558)**
    - **path-cost < 1 to 65535 >** -- Set port's path cost to the fixed value. **(p. 558)**
  - **point-to-point-mac < True | False | Auto >** -- Set the administrative point-to-point status. **(p. 560)**
  - **priority < 0 to 15 >** -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8). **(p. 564)**
  - **pvst-filter** -- Stop a specific port or ports from receiving and retransmitting PVST BPDUs. **(p. 565)**
  - **pvst-protection** -- Disable the specific port or ports if the port(s) receives PVST BPDUs. **(p. 565)**
  - **root-guard** -- Set port to ignore superior BPDUs to prevent it from becoming Root Port. **(p. 565)**
  - **tcn-guard** -- Set port to stop propagating received topology changes notifications and topology changes to other ports. **(p. 566)**
- spanning-tree **port-list** -- Configure the port-specific parameters of the spanning tree protocol for individual ports ([ethernet] PORT-LIST) **(p. 560)**
  - **mode < Norm | Fast | Uplink >** -- Set spanning tree operation mode. **(p. 558)**
  - **path-cost** -- Set port's path cost value. **(p. 558)**
    - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 554)**
    - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 558)**
    - **path-cost < 1 to 65535 >** -- Set port's path cost to the fixed value. **(p. 558)**
  - **priority < 0 to 255 >** -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8). **(p. 564)**
- spanning-tree **priority < 0 to 65535 >** -- Set the device STP priority. **(p. 564)**
- spanning-tree **priority < 0 to 15 >** -- Set the device STP priority (the value is in range of 0-61440 divided into steps of 4096 that are numbered from 0 to 15, default is step 8). **(p. 564)**
- [no] spanning-tree **trap < errant-bpdu >** -- Enable/disable STP traps. **(p. 566)**

COMMAND DETAILS

admin-edge-port

- [no] spanning-tree *[ETHERNET] PORT-LIST* admin-edge-port

```
Set the administrative edge port status.
```

apply

- spanning-tree pending apply

```
Apply pending MSTP configuration (swaps active and pending configuratons).
```

auto

- spanning-tree *[ETHERNET] PORT-LIST* path-cost auto

  ```
  Use dynamic method of selecting a value for the path cost.
  ```

- spanning-tree *[ETHERNET] PORT-LIST* path-cost auto

  ```
  Use dynamic method of selecting a value for the path cost.
  ```

- spanning-tree instance ist *[ETHERNET] PORT-LIST* path-cost auto

  ```
  Use dynamic method of selecting a value for the path cost.
  ```

- spanning-tree instance *< 1 to 16 >* *[ETHERNET] PORT-LIST* path-cost auto

  ```
  Use dynamic method of selecting a value for the path cost.
  ```

auto-edge-port

- [no] spanning-tree *[ETHERNET] PORT-LIST* auto-edge-port

  ```
  Set the automatic edge port detection.
  ```

bpdu-filter

- [no] spanning-tree *[ETHERNET] PORT-LIST* bpdu-filter

  ```
  Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a
   continuous fowarding state.
  ```

bpdu-protection

- [no] spanning-tree *[ETHERNET] PORT-LIST* bpdu-protection

  ```
  Disable the specific port or ports if the port(s) receives STP BPDUs.
  ```

bpdu-protection-timeout

- spanning-tree bpdu-protection-timeout *< 0 to 65535 >*

  ```
  Set the time for protected ports to be in down state after receiving unauthorized
  BPDUs.
  ```

  Range: < 0 to 65535 >

clear-debug-counters

- spanning-tree clear-debug-counters

  ```
  Clear spanning tree debug counters.
  ```

  Next Available Options:

  - **instance** < 0 to 16 > -- Clear spanning tree instance debug counters. (NUMBER) **(p. 556)**
  - **ports** -- Clear spanning tree port(s) debug counters. ([ethernet] PORT-LIST) **(p. 564)**

config-name

- [no] spanning-tree config-name

  ```
  Set the MST region configuration name (default is switch's MAC address).
  ```

  Next Available Option:

  - **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 555)**

- spanning-tree config-name *CONFIG-NAME*

  ```
  Specify the configuration name (maximum 32 characters).
  ```

- [no] spanning-tree pending config-name

  ```
  Set the pending MST region configuration name (default is switch's MAC address).
  ```

  Next Available Option:

  - **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 555)**

- spanning-tree pending config-name *CONFIG-NAME*

  ```
  Specify the configuration name (maximum 32 characters).
  ```

config-revision

- spanning-tree config-revision *< 0 to 65535 >*

  ```
  Set the MST region configuration revision number (default is 0).
  ```

  Range: < 0 to 65535 >

- spanning-tree pending config-revision *< 0 to 65535 >*

  ```
  Set the pending MST region configuration revision number (default is 0).
  ```

  Range: < 0 to 65535 >

force-version

- spanning-tree force-version *< STP-compatible | RSTP-operation >*

  ```
  Set Spanning Tree protocol compatibility mode.
  ```

  Supported Values:

  - **STP-compatible** -- The protocol operates as STP on all ports.
  - **RSTP-operation** -- The protocol operates as Rapid STP on all ports except those ports where a system that is using 802.1d Spanning Tree has been detected.

- spanning-tree force-version *< STP-compatible | RSTP-operation | MSTP-operation >*

  ```
  Set Spanning Tree protocol compatibility mode.
  ```

  Supported Values:

  - **STP-compatible** -- The protocol operates as STP on all ports.
  - **RSTP-operation** -- The protocol operates as Rapid STP on all ports except those ports where a system that is using 802.1d Spanning Tree has been detected.
  - **MSTP-operation** -- The protocol operates as Multiple STP on all ports where compatibility to the old STP protocol versions is not required.

forward-delay

- spanning-tree forward-delay *< 4 to 30 >*

```
Set time the switch waits between transitioning from listening to learning and from
learning to forwarding states.
```

Range: < 4 to 30 >

global

- spanning-tree *[ETHERNET] PORT-LIST* hello-time global

```
Use the globally configured hello-time value.
```

hello-time

- spanning-tree *[ETHERNET] PORT-LIST* hello-time

```
Set message transmission interval (in sec.) on the port.
```

Next Available Options:

- **hello-time** < 1 to 10 > -- Set message transmission interval (in sec.) on the port.**(p. 556)**
- **global** -- Use the globally configured hello-time value.**(p. 556)**

- spanning-tree *[ETHERNET] PORT-LIST* hello-time *< 1 to 10 >*

```
Set message transmission interval (in sec.) on the port.
```

Range: < 1 to 10 >

- spanning-tree hello-time *< 1 to 10 >*

```
Set time between messages transmission when the switch is root.
```

Range: < 1 to 10 >

instance

- spanning-tree instance

```
Usage: spanning-tree instance <ist|<1-16>> vlan VLAN-ID [VLAN-ID ...]
       [no] spanning-tree instance <1-16>
       [no] spanning-tree instance <ist|1-16> ...

Description: Create, delete or configure an MST instance.
             The first form of the command is used to create a new
             instance or map VLAN(s) to an existent one. Each instance
             must have at least one VLAN mapped to it. The VLANs
             unmapped from other instances are automatically mapped to
             the IST instance. Only IST VLANs can be directly mapped to
             other instances. When VLANs are mapped to an instance they
             are automatically unmapped from the instance they were
             mapped to before. Any MSTP instance can have all the VLANs
             configured in the switch. The second form of the command
             deletes an instance. The IST instance cannot be deleted. The
             third form of the command can be used to configure an existent
             instance. Follow the third form of the command with '?' to
             get a complete list of all the configurable parameters and
             sub-commands.
```

Next Available Options:

- **ist** -- Configure internal spanning tree (IST) instance.**(p. 557)**
- **MSTID** < 1 to 16 > -- ID of the MST instance to configure.**(p. 558)**

- spanning-tree pending instance

```
Change pending MST instance configuration.
```

Next Available Option:

- **MSTID** < 1 to 16 > -- ID of the MST instance to configure.**(p. 558)**

- spanning-tree clear-debug-counters instance *< 0 to 16 >*

```
Clear spanning tree instance debug counters.
```

Range: < 0 to 16 >

Next Available Option:

- **ports** -- Clear spanning tree port(s) debug counters. ([ethernet] PORT-LIST) **(p. 564)**

- spanning-tree clear-debug-counters ports *[ETHERNET] PORT-LIST* instance *< 0 to 16 >*

```
Clear spanning tree instance debug counters.
```

Range: < 0 to 16 >

ist

- spanning-tree instance ist

```
Configure internal spanning tree (IST) instance.
```

Next Available Option:

- **port-list** -- Configure internal spanning tree (IST) instance ports parameters ([ethernet] PORT-LIST) **(p. 560)**

legacy-mode

- [no] spanning-tree legacy-mode

```
Set spanning-tree protocol to operate either in 802.1D legacy
mode or in 802.1s native mode.
'spanning-tree legacy-mode' is the equivalent of executing:
     spanning-tree legacy-path-cost
     spanning-tree force-version stp-compatible
'no spanning-tree legacy-mode' is the equivalent of executing:
     no spanning-tree legacy-path-cost
     spanning-tree force-version mstp-operation
```

legacy-path-cost

- [no] spanning-tree legacy-path-cost

```
Set 802.1D (legacy) or 802.1t (not legacy) default pathcost values.
```

max-hops

- spanning-tree max-hops *< 1 to 40 >*

  ```
  Set the max number of hops in a region before the MST BPDU is discarded and the
  information held for a port is aged (default is 20).
  ```

  Range: < 1 to 40 >

maximum-age

- spanning-tree maximum-age *< 6 to 40 >*

  ```
  Set maximum age of received STP information before it is discarded.
  ```

  Range: < 6 to 40 >

mcheck

- spanning-tree *[ETHERNET] PORT-LIST* mcheck

  ```
  Force the port to transmit RST BPDUs.
  ```

mode

- spanning-tree *[ETHERNET] PORT-LIST* mode *< Norm | Fast | Uplink >*

  ```
  Set spanning tree operation mode.
  ```

  Supported Values:
  - **Norm** -- Normal spanning tree mode.
  - **Fast** -- Fast spanning tree mode.
  - **Uplink** -- Fast Uplink spanning tree mode.

MSTID

- [no] spanning-tree instance *< 1 to 16 >*

  ```
  ID of the MST instance to configure.
  ```

  Range: < 1 to 16 >

  Next Available Options:
  - **vlan** -- Configure VLANs for the MST instance.**(p. 566)**
  - **priority** < 0 to 15 > -- Set the device priority for the MST instance (the value is in range of 0-61440 divided into steps of 4096 that are numbered from 0 to 15, default is step 8).**(p. 564)**
  - **port-list** -- Configure MST instance ports parameters ([ethernet] PORT-LIST) **(p. 560)**

- [no] spanning-tree pending instance *< 1 to 16 >*

  ```
  ID of the MST instance to configure.
  ```

  Range: < 1 to 16 >

  Next Available Option:
  - **vlan** -- Configure VLANs for the MST instance.**(p. 566)**

path-cost

- spanning-tree *[ETHERNET] PORT-LIST* path-cost

```
Set port's path cost value.
```

Next Available Options:

- **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 558)**
- **path-cost** < 1 to 65535 > -- Set port's path cost to the fixed value.**(p. 558)**
- **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 554)**

- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

  ```
  Set port's path cost to the fixed value.
  ```

  Range: < 1 to 200000000 >
- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 65535 >*

  ```
  Set port's path cost to the fixed value.
  ```

  Range: < 1 to 65535 >
- spanning-tree *[ETHERNET] PORT-LIST* path-cost

  ```
  Set port's path cost value.
  ```

  Next Available Options:

  - **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 558)**
  - **path-cost** < 1 to 65535 > -- Set port's path cost to the fixed value.**(p. 558)**
  - **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 554)**

- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

  ```
  Set port's path cost to the fixed value.
  ```

  Range: < 1 to 200000000 >
- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 65535 >*

  ```
  Set port's path cost to the fixed value.
  ```

  Range: < 1 to 65535 >
- spanning-tree instance ist *[ETHERNET] PORT-LIST* path-cost

  ```
  Set the internal port pathcost for the IST (default is 'auto').
  ```

  Next Available Options:

  - **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 558)**
  - **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 554)**

- spanning-tree instance ist *[ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

  ```
  Set port's path cost to the fixed value.
  ```

  Range: < 1 to 200000000 >
- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* path-cost

  ```
  Set the port pathcost for the instance (default is 'auto').
  ```

  Next Available Options:

  - **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 558)**

  - **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 554)**

- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

  ```
  Set port's path cost to the fixed value.
  ```

  Range: < 1 to 200000000 >

pending

- spanning-tree pending

  ```
  Usage: spanning-tree pending <apply|reset>
         [no] spanning-tree pending [...]

  Description: Manipulate pending MSTP configuration. The pending
               configuration can be modified without affecting current
               spanning tree operation. The 'spanning-tree pending apply'
               command runs the pending configuration consistency check
               and activates the pending configuration if it yields no
               consistency errors. The pending and active configurations
               exchange places if the 'apply' command is completed
               successfully.
               The 'spanning-tree pending reset' command overrides pending
               configuration with the active one.
               Not all spanning tree parameters are available for the pending
               configuration. The parameters that are not available for the
               pending configuration are not affected or when must be
               implicitly set are initialized to the defaults. Use
               'spanning-tree pending ?' to get a complete list of all
               supported pending configuration commands and parameters.
  ```

  Next Available Options:

  - **apply** -- Apply pending MSTP configuration (swaps active and pending configuratons).**(p. 553)**
  - **reset** -- Copy active configuration to pending.**(p. 565)**
  - **config-name** -- Set the pending MST region configuration name (default is switch's MAC address).**(p. 555)**
  - **config-revision** < 0 to 65535 > -- Set the pending MST region configuration revision number (default is 0).**(p. 555)**
  - **instance** -- Change pending MST instance configuration.**(p. 556)**

point-to-point-mac

- spanning-tree *[ETHERNET] PORT-LIST* point-to-point-mac *< True | False | Auto >*

  ```
  Set the administrative point-to-point status.
  ```

  Supported Values:

  - **True** -- Treat the port as if it is connected to a point-to-point LAN segment.
  - **False** -- Treat the port as if it is connected to a non-point-to-point LAN segment.
  - **Auto** -- Determine automatically status of the segment connected to the port.

port-list

- [no] spanning-tree *[ETHERNET] PORT-LIST*

  ```
  Usage: spanning-tree [ethernet] PORT-LIST <<admin-edge-port>|auto-edge-port>|
                                  <mcheck>|
  ```

```
                            <path-cost <1-65535>|<1-200000000>|auto>>|
                            <point-to-point <true|false|auto>>|
                            <bpdu-filter>|
                            <bpdu-protection>|
                            <pvst-filter>|
                            <pvst-protection>|
                            <root-guard> | <tcn-guard>|
                            <hello-time <1-10>>|
                            <priority <0-15>>>

Description: Configure the port-specific parameters of the spanning
             tree protocol for individual ports.

Parameters:
    o admin-edge-port - Applies only to RSTP/MSTP. When correctly set for each
      port it improves the protocol operation. Indicate whether the port is
      connected to LAN segment that doesn't have any bridge or switch
      connected to it. If a bridge or switch is detected on the segment,
      the port will automatically operate as if Edge = 'No' has been set.
    o auto-edge-port - Applies only to MSTP. Used to set the automatic edge
      port detection.
    o mcheck - Applies only to RSTP/MSTP. Forces the Port Protocol Migration
      state machine to transmit RST or MST BPDUs for a Migrate Time period
      to test whether all STP Bridges on the attached LAN have been removed
      and the port can continue to transmit RST or MST BPDUs. Setting mcheck
      has no effect if the Bridge is operating in STP Compatibility mode.
    o path-cost <1-65535> or <1-200000000> or <auto> - Individual port cost -
      used to determine which ports are forwarding ports.
      Can be set to 'auto' or configured by a user. A value of 'auto' (default)
      indicates the link speed determines the cost value. The following ranges
      are available for user configuration:
      For RSTP/MSTP: 1 through 200000000 (recommended value is 2000000 for
      Ethernet and 10/100TX ports operating at 10 Mbps; 200000 for 10/100TX
      ports operating at 100 Mbps and 100FX; 20000 for 1000SX, 1000LX,
      1000Stk, 1000T ports).
      For STP: 1 through 65535 (recommended value is 100 for Ethernet and
      10/100TX ports operating at 10 Mbps; 10 for 10/100TX ports operating
      at 100 Mbps and 100FX; 5 for 1000SX, 1000LX, 1000Stk, 1000T ports).
    o pvst-filter (default: off) - On/off control to ignore a port's
      incoming per-VLAN spanning tree (PVST) BPDU packets.
    o pvst-protection (default: disabled) - Enable/Disable per-VLAN
      spanning tree (PVST) protection on port(s).  If pvst-protection
      is enabled on specified port(s) and if the port(s) receive
      PVST BPDU packets then the port(s) will be disabled
      If enabled, this takes precendence over the pvst-filter
     configuration for a port.   o root-guard - Applies only to MSTP. If TRUE causes
 the port not to be
      selected as Root Port for the CIST or any MSTI.
    o tcn-guard - Applies only to MSTP. If TRUE causes the port not to
      propagate received topology notifications and topology changes to
      other ports.
    o bpdu-filter (default: off) - On/off control to ignore a port's
      incoming spanning-tree BPDU packets and prevent sending any.
    o bpdu-protection (default: disabled) - Enable/Disable STP BPDU
      protection on port(s). If bpdu-protection is enabled on specified
      port(s) and if the port(s) receives spanning-tree BPDU packets then
      the port(s) will be disabled.
    o point-to-point <true|false|auto> (default: auto) - Applies only to
      RSTP/MSTP. When correctly set for each port, it improves the operation
      of protocol. 'True' indicates that the port will be treated as if it is
```

```
            connected to a point-to-point LAN segment, regardless of any information
            to the contrary that the switch receives. 'False' indicates that
            the port will be treated as if it is connected to a non-point-to-point
            LAN segment, regardless of any information to the contrary that the
            switch receives. Set 'False' on any port that is known to be
            connected to a hub, bridge, or another switch. 'Auto' value indicates
            that the administrator requires the point-to-point status of the MAC
            to be determined in accordance with the specific MAC procedures.
          o priority <0-15> (default: 8 ) -  Another value used by spanning tree
            to select the forwarding ports. The port with the lowest number has
            the highest priority. The range of 0-240 is divided into 16 steps. These
            steps are numbered from 0 to 15. The number entered is multiplied to 16
            to calculate the priority value to use by the protocol if protocol
            version is other than standard STP (802.1D).
          o hello-time <<1-10>|global> (default: global) - Time (in seconds)
            between message transmissions when the switch is root. Available for
            the per-port configuration in MSTP mode only. The value 'global' means
            to use globally configured hello-time for the port.
```

Next Available Options:

- **admin-edge-port** -- Set the administrative edge port status.**(p. 553)**
- **auto-edge-port** -- Set the automatic edge port detection.**(p. 554)**
- **mcheck** -- Force the port to transmit RST BPDUs.**(p. 558)**
- **path-cost** -- Set port's path cost value.**(p. 558)**
- **point-to-point-mac** < True | False | Auto > -- Set the administrative point-to-point status.**(p. 560)**
- **priority** < 0 to 15 > -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8).**(p. 564)**
- **hello-time** -- Set message transmission interval (in sec.) on the port.**(p. 556)**
- **root-guard** -- Set port to ignore superior BPDUs to prevent it from becoming Root Port.**(p. 565)**
- **tcn-guard** -- Set port to stop propagating received topology changes notifications and topology changes to other ports.**(p. 566)**
- **bpdu-filter** -- Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a continuous fowarding state.**(p. 554)**
- **bpdu-protection** -- Disable the specific port or ports if the port(s) receives STP BPDUs.**(p. 554)**
- **pvst-protection** -- Disable the specific port or ports if the port(s) receives PVST BPDUs.**(p. 565)**
- **pvst-filter** -- Stop a specific port or ports from receiving and retransmitting PVST BPDUs.**(p. 565)**

- spanning-tree *[ETHERNET] PORT-LIST*

```
Usage: spanning-tree [ethernet] PORT-LIST <<admin-edge-port>|auto-edge-port>|
                            <mcheck>|
                            <path-cost <1-65535>|<1-200000000>|auto>>|
                            <point-to-point <true|false|auto>>|
                            <bpdu-filter>|
                            <bpdu-protection>|
                            <pvst-filter>|
                            <pvst-protection>|
                            <root-guard> | <tcn-guard>|
                            <hello-time <1-10>>|
                            <priority <0-15>>>

Description: Configure the port-specific parameters of the spanning
             tree protocol for individual ports.

Parameters:
    o admin-edge-port - Applies only to RSTP/MSTP. When correctly set for each
      port it improves the protocol operation. Indicate whether the port is
      connected to LAN segment that doesn't have any bridge or switch
      connected to it. If a bridge or switch is detected on the segment,
      the port will automatically operate as if Edge = 'No' has been set.
    o auto-edge-port - Applies only to MSTP. Used to set the automatic edge
      port detection.
    o mcheck - Applies only to RSTP/MSTP. Forces the Port Protocol Migration
      state machine to transmit RST or MST BPDUs for a Migrate Time period
      to test whether all STP Bridges on the attached LAN have been removed
      and the port can continue to transmit RST or MST BPDUs. Setting mcheck
      has no effect if the Bridge is operating in STP Compatibility mode.
    o path-cost <1-65535> or <1-200000000> or <auto> - Individual port cost -
      used to determine which ports are forwarding ports.
      Can be set to 'auto' or configured by a user. A value of 'auto' (default)
      indicates the link speed determines the cost value. The following ranges
      are available for user configuration:
      For RSTP/MSTP: 1 through 200000000 (recommended value is 2000000 for
      Ethernet and 10/100TX ports operating at 10 Mbps; 200000 for 10/100TX
      ports operating at 100 Mbps and 100FX; 20000 for 1000SX, 1000LX,
      1000Stk, 1000T ports).
      For STP: 1 through 65535 (recommended value is 100 for Ethernet and
      10/100TX ports operating at 10 Mbps; 10 for 10/100TX ports operating
      at 100 Mbps and 100FX; 5 for 1000SX, 1000LX, 1000Stk, 1000T ports).
    o pvst-filter (default: off) - On/off control to ignore a port's
      incoming per-VLAN spanning tree (PVST) BPDU packets.
    o pvst-protection (default: disabled) - Enable/Disable per-VLAN
      spanning tree (PVST) protection on port(s).  If pvst-protection
      is enabled on specified port(s) and if the port(s) receive
      PVST BPDU packets then the port(s) will be disabled
      If enabled, this takes precendence over the pvst-filter
     configuration for a port.    o root-guard - Applies only to MSTP. If TRUE causes
 the port not to be
      selected as Root Port for the CIST or any MSTI.
    o tcn-guard - Applies only to MSTP. If TRUE causes the port not to
      propagate received topology notifications and topology changes to
      other ports.
    o bpdu-filter (default: off) - On/off control to ignore a port's
      incoming spanning-tree BPDU packets and prevent sending any.
    o bpdu-protection (default: disabled) - Enable/Disable STP BPDU
      protection on port(s). If bpdu-protection is enabled on specified
      port(s) and if the port(s) receives spanning-tree BPDU packets then
      the port(s) will be disabled.
    o point-to-point <true|false|auto> (default: auto) - Applies only to
      RSTP/MSTP. When correctly set for each port, it improves the operation
      of protocol. 'True' indicates that the port will be treated as if it is
      connected to a point-to-point LAN segment, regardless of any information
      to the contrary that the switch receives. 'False' indicates that
      the port will be treated as if it is connected to a non-point-to-point
      LAN segment, regardless of any information to the contrary that the
      switch receives. Set 'False' on any port that is known to be
      connected to a hub, bridge, or another switch. 'Auto' value indicates
      that the administrator requires the point-to-point status of the MAC
      to be determined in accordance with the specific MAC procedures.
    o priority <0-15> (default: 8 ) -  Another value used by spanning tree
      to select the forwarding ports. The port with the lowest number has
      the highest priority. The range of 0-240 is divided into 16 steps. These
      steps are numbered from 0 to 15. The number entered is multiplied to 16
      to calculate the priority value to use by the protocol if protocol
      version is other than standard STP (802.1D).
    o hello-time <<1-10>|global> (default: global) - Time (in seconds)
      between message transmissions when the switch is root. Available for
      the per-port configuration in MSTP mode only. The value 'global' means
      to use globally configured hello-time for the port.
```

Next Available Options:

- **mode** < Norm | Fast | Uplink > -- Set spanning tree operation mode.**(p. 558)**
- **path-cost** -- Set port's path cost value.**(p. 558)**
- **priority** < 0 to 255 > -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8).**(p. 564)**

- spanning-tree instance ist *[ETHERNET] PORT-LIST*

```
Usage: spanning-tree ist [ethernet] PORT-LIST ...

Description: Configure internal spanning tree (IST) instance ports parameters.
             Follow the PORT-LIST with the '?' to get the list of all
             possible options.
```

Next Available Option:

- **path-cost** -- Set the internal port pathcost for the IST (default is 'auto').**(p. 558)**

- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST*

```
Usage: spanning-tree instance <1-16> [ethernet] PORT-LIST ...

Description: Configure MST instance ports parameters. Follow the PORT-LIST
             with the '?' to get the list of all possible options.
```

Next Available Options:

- **path-cost** -- Set the port pathcost for the instance (default is 'auto').**(p. 558)**
- **priority** < 0 to 15 > -- Set the port priority for the instance (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8).**(p. 564)**

ports

- spanning-tree clear-debug-counters instance *< 0 to 16 >* ports *[ETHERNET] PORT-LIST*

```
Clear spanning tree port(s) debug counters.
```

- spanning-tree clear-debug-counters ports *[ETHERNET] PORT-LIST*

```
Clear spanning tree port(s) debug counters.
```

Next Available Option:

- **instance** < 0 to 16 > -- Clear spanning tree instance debug counters. (NUMBER) **(p. 556)**

priority

- spanning-tree *[ETHERNET] PORT-LIST* priority *< 0 to 15 >*

```
Set port priority (the value is in range of 0-240 divided into steps of 16 that are
numbered from 0 to 15, default is step 8).
```

Range: < 0 to 15 >

- spanning-tree *[ETHERNET] PORT-LIST* priority *< 0 to 255 >*

  ```
  Set port priority (the value is in range of 0-240 divided into steps of 16 that are
  numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 255 >

- spanning-tree priority *< 0 to 65535 >*

  ```
  Set the device STP priority.
  ```

  Range: < 0 to 65535 >

- spanning-tree priority *< 0 to 15 >*

  ```
  Set the device STP priority (the value is in range of 0-61440 divided into steps of
  4096 that are numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >

- spanning-tree instance *< 1 to 16 >* priority *< 0 to 15 >*

  ```
  Set the device priority for the MST instance (the value is in range of 0-61440 divided
   into steps of 4096 that are numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >

- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* priority *< 0 to 15 >*

  ```
  Set the port priority for the instance (the value is in range of 0-240 divided into
  steps of 16 that are numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >

pvst-filter

- [no] spanning-tree *[ETHERNET] PORT-LIST* pvst-filter

  ```
  Stop a specific port or ports from receiving and retransmitting PVST BPDUs. The command
   indicates
  which ports are not expected to receive any PVST BPDUs.

  Default: Disabled on all ports.
  ```

pvst-protection

- [no] spanning-tree *[ETHERNET] PORT-LIST* pvst-protection

  ```
  Enables or disables the PVST protection feature on the port or range of ports specified.
   The
  command indicates which ports are not expected to receive any PVST BPDUs.

  Default: Disabled on all ports
  ```

reset

- spanning-tree pending reset

  ```
  Copy active configuration to pending.
  ```

root-guard

- [no] spanning-tree *[ETHERNET] PORT-LIST* root-guard

```
Set port to ignore superior BPDUs to prevent it from becoming Root Port.
```

tcn-guard

- [no] spanning-tree *[ETHERNET] PORT-LIST* tcn-guard

  ```
  Set port to stop propagating received topology changes notifications
   and topology changes to other ports.
  ```

trap

- [no] spanning-tree trap *< errant-bpdu >*

  ```
  Enable/disable STP traps.
  ```

  Supported Values:
  - **errant-bpdu**

vlan

- spanning-tree instance *< 1 to 16 >* vlan

  ```
  Configure VLANs for the MST instance.
  ```

  Next Available Option:
  - **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 566)**

- spanning-tree pending instance *< 1 to 16 >* vlan

  ```
  Configure VLANs for the MST instance.
  ```

  Next Available Option:
  - **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 566)**

VLAN-ID-RANGE

- [no] spanning-tree instance *< 1 to 16 >* vlan *VLAN-ID-RANGE*

  ```
  VLAN(s) to add to or to remove from the MST instance
  ```

- [no] spanning-tree pending instance *< 1 to 16 >* vlan *VLAN-ID-RANGE*

  ```
  VLAN(s) to add to or to remove from the MST instance
  ```

stack

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage:  [no] stack
        [no] stack commander ASCII-STR
        [no] stack join MAC-ADDR
        [no] stack member INTEGER mac-address MAC-ADDR [password ASCII-STR]
        [no] stack auto-join
        [no] stack auto-grab
             stack transmission-interval <1-300>

Description: Configure device to/from a stack - a group of devices manageable
             as a single entity.
          -  'stack' by itself enables stacking on the switch. The 'no' option
             disables stacking.
          -  'stack commander' configures the switch to be a 'commander switch'
             given the name specified in the ASCII-STR parameter. The 'no'
             option disables the commander function. The 'commander switch' can
             be used as a single point of access for configuring and monitoring
             all the switches in the stack.
          -  'stack join' causes the switch, as a candidate switch, to join the
             stack whose commander switch is identified by the MAC-ADDR
             parameter. The 'no' option causes the switch to leave that stack.
          -  'stack member' causes a candidate switch identified by the
             MAC-ADDR to be an INTEGER-th member of this switch's stack in case
             of this switch is a commander. The INTEGER number must be between
             1 and 15 (0 is reserved for the commander switch). Password must
             be supplied if the candidate switch has a manager password.
          -  'stack auto-join' allows this switch, being a candidate, to
             automatically join a stack. The 'no' option disables this feature.
          -  'stack auto-grab' allows this switch, being a commander, to
             automatically incorporate candidates. The 'no' option disables
             this feature.
          -  'stack transmission-interval' sets the transmission-interval (in
             seconds) between the sending out of new discovery packets. The
             default value is 60 seconds.
```

COMMAND STRUCTURE

- [no] stack **auto-grab** -- Configure commander to incorporate candidates **(p. 568)**
- [no] stack **auto-join** -- Allow this switch to automatically join a stack **(p. 568)**
- [no] stack **commander** -- Configure this switch to be a commander (ASCII-STR) **(p. 568)**
- [no] stack **join** -- Join a stack as a member (MAC-ADDR) **(p. 568)**
- [no] stack **member** -- Incorporate candidate into stack **(p. 568)**
  - **mac-address** -- MAC address of candidate (MAC-ADDR) **(p. 568)**
  - **password** -- Manager password of candidate (ASCII-STR) **(p. 568)**
- stack **transmission-interval** **< 1 to 300 >** -- Transmission interval of HP discovery packets **(p. 568)**

COMMAND DETAILS

auto-grab

- [no] stack auto-grab

```
Configure commander to incorporate candidates
```

auto-join

- [no] stack auto-join

```
Allow this switch to automatically join a stack
```

commander

- [no] stack commander *COMMANDER*

```
Configure this switch to be a commander
```

join

- [no] stack join *MAC-ADDR*

```
Join a stack as a member
```

mac-address

- stack member *INTEGER* mac-address *MAC-ADDR*

```
MAC address of candidate
```

member

- [no] stack member *INTEGER*

```
Incorporate candidate into stack
```

Next Available Options:

- **mac-address** -- MAC address of candidate (MAC-ADDR) **(p. 568)**
- **password** -- Manager password of candidate (ASCII-STR) **(p. 568)**

password

- stack member *INTEGER* password *PASSWORD*

```
Manager password of candidate
```

transmission-interval

- stack transmission-interval *< 1 to 300 >*

```
Transmission interval of HP discovery packets
```

Range: < 1 to 300 >

startup-default

OVERVIEW

Category:	manager
Primary context:	manager
Related Commands	show config (page 462) show flash (page 472)

```
Usage: startup-default [<primary|secondary>] config FILENAME

Description: Set the default configuration file.  A separate configuration
             file may be set as the default for each software image, or a
             single configuration file may be set as the default when
             booting either image by omitting the optional 'primary|secondary'
             parameter.
```

COMMAND STRUCTURE

- startup-default config **< config | new >** -- Specify configuration file to set as default. (p. 569)
- startup-default image **< primary | secondary >** -- (p. 569)
  - config **< config | new >** -- Specify configuration file to set as default. (p. 569)

COMMAND DETAILS

config (p. 569)	image (p. 569)

config

- startup-default *< primary | secondary >* config *< config | new >*

  ```
  Specify configuration file to set as default.
  ```

  Supported Values:
  - **config**
  - **new**
- startup-default config *< config | new >*

  ```
  Specify configuration file to set as default.
  ```

  Supported Values:
  - **config**
  - **new**

image

- startup-default *< primary | secondary >*

  Supported Values:
  - **primary** -- Primary flash image.
  - **secondary** -- Secondary flash image.

  Next Available Option:
  - config < config | new > -- Specify configuration file to set as default.(p. 569)

static-mac

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show static-mac (page 510)**

```
Usage: static-mac <MAC-ADDR> vlan <VLAN-ID> interface <PORT-LIST>

Description: Lock down a MAC address to a port on a vlan.

Parameters:

    o MAC-ADDR  - MAC address to lock down.

    o vlan VLAN-ID - VLAN on which to lock down the MAC address.

    o interface PORT-LIST - Port list on which to lock down the MAC address.

Examples:

    (1) hp-switch#  static-mac 0800095F3AD6 vlan V1 interface A1
```

COMMAND STRUCTURE

- [no] static-mac MAC-ADDR **interface** -- The port list on which to lock down the MAC address. ([ethernet] PORT-NUM) **(p. 570)**
- [no] static-mac MAC-ADDR **vlan** -- The VLAN ID on which to lock down the MAC address. (VLAN-ID) **(p. 570)**

EXAMPLES

Example: static-mac MAC-ADDR <...>

Lock MAC address 0800095F3AD6 to port A1 on VLAN V1:

```
ProCurve# static-mac 0800095F3AD6 vlan V1 interface A1
```

COMMAND DETAILS

interface (p. 570)	**vlan (p. 570)**

interface

- [no] static-mac *MAC-ADDR* interface *[ETHERNET] PORT-NUM*

```
The port list on which to lock down the MAC address.
```

vlan

- [no] static-mac *MAC-ADDR* vlan *VLAN-ID*

```
The VLAN ID on which to lock down the MAC address.
```

static-vlan

OVERVIEW

Category:	config
Primary context:	config
Related Commands	show vlan (page 518) show gvrp (page 474) gvrp (page 180)

```
Usage: static-vlan VLAN-ID
```

```
Description: Transform a dynamic VLAN to a static VLAN.
```

COMMAND STRUCTURE

EXAMPLES

Example: static-vlan

Convert dynamically created VLAN 125 into a port-based, static VLAN:

```
ProCurve(config)# static-vlan 125
```

svlan

OVERVIEW

Category:	
Primary context:	config
Related Commands	qinq (page 380) vlan (page 611) show qinq (page 500) show svlans (page 512)

```
Usage: [no] svlan VLAN-ID [...]

Description: Add, delete, edit SVLAN configuration or enter a SVLAN context.
             If an existing 'SVLAN VLAN-ID' is specified you are put into the
             context for that SVLAN, and can then execute commands for that
             SVLAN. If a new VLAN-ID is specified, the new SVLAN is added with
             the VLAN-ID, and you are put into the context of the new SVLAN.
             If you follow the command with one of the SVLAN Context commands
             in the same command line, the context level is not changed, but
             the commands are executed for the SVLAN specified by the
             VLAN-ID.
             The 'no' option of the SVLAN command is used to delete
             the SVLAN specified by VLAN-ID. If one or more ports belong only
             to the S-VLAN to be deleted, the CLI notifies you that these ports
             will be moved to the default VLAN and prompts you to continue the
             deletion.
```

NOTES

SVLANS

S-VLANS are used to tunnel customer frames throught the provider network to customer sites. These are managed by the service provider who can assign each customer a unique S-VLAN_ID.

COMMAND STRUCTURE

- svlan VLAN-ID **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 576)**
- svlan VLAN-ID **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter **(p. 576)**
  - **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 583)**
    - **all** -- Resets all previously blocked by the connection rate filter **(p. 576)**
    - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 578)**
    - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 583)**
- [no] svlan VLAN-ID **dhcp-snooping** -- **(p. 577)**
- [no] svlan VLAN-ID **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 578)**
- [no] svlan VLAN-ID **ip** -- Configure various IP parameters for the VLAN **(p. 578)**
  - **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 574)**
    - **direction < in | out | connection-rate-filter | ... >** -- **(p. 577)**
  - **address** -- Set IP parameters for communication within an IP network **(p. 574)**

        - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 577)**
        - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 579)**
- [no] svlan VLAN-ID **ipv6** -- Configure various IP parameters for the VLAN **(p. 579)**
    - **address** -- Set IPv6 parameters for communication within an IP network **(p. 574)**
        - **autoconfig** -- Automatic address configuration. **(p. 576)**
        - **dhcp** -- Configure a DHCPv6 client. **(p. 577)**
            - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server. **(p. 578)**
                - **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server. **(p. 583)**
        - **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 579)**
            - **link-local** -- Configure a link-local IPv6 address. **(p. 580)**
        - **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 579)**
            - **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes **(p. 576)**
            - **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface **(p. 578)**
    - **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr. **(p. 577)**
- [no] svlan VLAN-ID **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size **(p. 579)**
- [no] svlan VLAN-ID **monitor** -- Define either the VLAN is to be monitored or not **(p. 580)**
    - **all < In | Out | Both >** -- Monitor all traffic. **(p. 576)**
        - **mirror** -- Mirror destination. **(p. 580)**
            - **mirror_session_name** -- Mirror destination name. **(p. 580)**
            - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 581)**
    - **ip** -- Apply an IPv4 access list. **(p. 578)**
        - **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 574)**
            - **monitor_mirror_ACL_dir < In >** -- Define the mirror port for diagnostic purposes **(p. 581)**
                - **mirror** -- Mirror destination. **(p. 580)**
                    - **mirror_session_name** -- Mirror destination name. **(p. 580)**
                    - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 581)**
- svlan VLAN-ID **name** -- Set the VLAN's name (ASCII-STR) **(p. 581)**
- [no] svlan VLAN-ID **protocol** -- Set a predefined protocol for the current VLAN. **(p. 582)**
    - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 582)**
    - **protocols < IPX | IPv4 | IPv6 | ... >** -- Set a predefined protocol for the current VLAN. **(p. 582)**
- [no] svlan VLAN-ID **qos** -- Set VLAN-based priority **(p. 582)**
    - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 577)**
    - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 581)**
- [no] svlan VLAN-ID **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 583)**
- [no] svlan VLAN-ID **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 583)**
- [no] svlan VLAN-ID **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network **(p. 583)**

COMMAND DETAILS

access-group (p. 574)
address (p. 574)
all (p. 576)
anycast (p. 576)
forbid (p. 578)
full (p. 578)
host (p. 578)
ip (p. 578)
monitor_mirror_session_id (p. 581)
name (p. 581)
priority (p. 581)

access-group

- [no] svlan *VLAN-ID* ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> <in|out>

in                     Match packets this device will route to another VLAN
out                    Match packets this device will route onto this VLAN
vlan                   Match packets that originate within this VLAN
connection-rate-filter Manage new conection rates originating in this VLAN

   Description: Apply the specified access control list on this VLAN interface.
                The ACL can match either packets that are routed from this VLAN
                to another VLAN, packets that will be routed from another VLAN
                to this VLAN, packets that originate on this VLAN, or it can
                manage new connection rates for virus throttling.
```

Next Available Option:

- **direction** < in | out | connection-rate-filter | ... > -- **(p. 577)**

- svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:

- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 581)**

address

- [no] svlan *VLAN-ID* ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.
             Each VLAN represents an IP interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ip address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:

    o dhcp-bootp - The switch attempts to get its configuration from a
      DHCP/Bootp server.

    o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch or VLAN.
      The IP-ADDR/MASK-LENGTH may be specified in two ways using the
      following syntax:
          ip address 192.32.36.87/24
          ip address 192.32.36.87 255.255.255.0
      Both of the statements above would have the same effect.
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 579)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 577)**

- [no] svlan *VLAN-ID* ipv6 address

```
Usage: [no] ipv6 address [dhcp|autoconfig|IPv6-ADDR/PREFIX-LEN]

Description: Set IPv6 parameters for communication within an IP network.
             Each VLAN represents an IPv6 interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ipv6 address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:
    o autoconfig - Enables automatic address configuration of IPv6
      addresses using stateless configuration of an interface .

    o dhcp - The switch attempts to get its configuration from a
      DHCPv6 server.

    o IPv6-ADDR/PREFIX-LEN-Assign an IPv6 address to the switch or VLAN.
      The IPv6-ADDR/PREFIX-LEN may be specified in four ways using the
      following syntax:
          ipv6 address 1234:abcd::5678/40
          ipv6 address 2001:0db8:1:1:ffff:ffff:ffff:fffe/64 anycast
          ipv6 address 2001:0db8:0:1::/64 eui-64
      Only link-local addreses are configured without PREFIX-LEN as below:
          ipv6 address FE80:0:0:0:0123:0456:0789:0abc link-local
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **autoconfig** -- Automatic address configuration.**(p. 576)**
- **dhcp** -- Configure a DHCPv6 client.**(p. 577)**
- **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 579)**
- **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 579)**

all

- svlan *VLAN-ID* connection-rate-filter unblock all

```
Resets all previously blocked by the connection rate filter
```

- svlan *VLAN-ID* monitor all *< In | Out | Both >*

```
Monitor all traffic.
```

Supported Values:

- **In** -- Monitor all inbound traffic
- **Out** -- Monitor all outbound traffic
- **Both** -- Monitor all inbound and outbound traffic

Next Available Option:

- **mirror** -- Mirror destination.**(p. 580)**

anycast

- [no] svlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* anycast

```
Address that is assigned to a set of interfaces that typically belong to different
nodes
```

auto

- svlan *VLAN-ID* auto *[ETHERNET] PORT-LIST*

```
Usage: [no] auto [ethernet] PORT-LIST

Description: Cause each port identified in the port list to learn its
             VLAN membership using the GARP VLAN Registration Protocol
             (GVRP). This command is only valid when GVRP is enabled.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

autoconfig

- [no] svlan *VLAN-ID* ipv6 address autoconfig

```
Automatic address configuration.
```

connection-rate-filter

- svlan *VLAN-ID* connection-rate-filter

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK >

       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Re-enables access to a host or set of hosts  that has been previously
             blocked by the connection rate filter. Disabling or setting sensitivity

             may have improved performance after rebooting the switch
```

Next Available Option:

- **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 583)**

dhcp

- [no] svlan *VLAN-ID* ipv6 address dhcp

```
Configure a DHCPv6 client.
```

Next Available Option:

- **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server.**(p. 578)**

dhcp-bootp

- svlan *VLAN-ID* ip address dhcp-bootp

```
Configure the interface to use DHCP/Bootp server to acquire parameters.
```

dhcp-snooping

- [no] svlan *VLAN-ID* dhcp-snooping

direction

- [no] svlan *VLAN-ID* ip access-group *ACCESS-GROUP < in | out | connection-rate-filter | ... >*

Supported Values:

- **in** -- Match inbound packets
- **out** -- Match outbound packets
- **connection-rate-filter** -- Manage packet rates
- **vlan** -- VLAN acl

dscp

- svlan *VLAN-ID* qos dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

Supported Values:

Binary formatted value from 000000 to 111111

enable

- [no] svlan *VLAN-ID* ipv6 enable

```
Enable IPv6 on an interface and configures an automatically generated link-local addr.
```

eui-64

- [no] svlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* eui-64

```
An IPv6 EUI-64 address that can be automatically configured on any interface
```

forbid

- [no] svlan *VLAN-ID* forbid *[ETHERNET] PORT-LIST*

```
Usage: [no] forbid [ethernet] PORT-LIST

Description: Prevent ports from becoming a member of the current VLAN.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

full

- [no] svlan *VLAN-ID* ipv6 address dhcp full

```
Obtain IPv6 address & Configuration information from DHCPv6 server.
```

Next Available Option:

- **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server.**(p. 583)**

host

- svlan *VLAN-ID* connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

ip

- svlan *VLAN-ID* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the VLAN. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 574)**
- **address** -- Set IP parameters for communication within an IP network**(p. 574)**

- [no] svlan *VLAN-ID* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:

- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 574)**

ip-addr

- [no] svlan *VLAN-ID* ip address *IP-ADDR/MASK-LENGTH*

```
Interface IP address/mask.
```

ipv6

- svlan *VLAN-ID* ipv6

```
Usage: [no] ipv6 ...

Description: Configure various IP parameters for the VLAN. The 'ipv6'
             command must be followed by a feature-specific keyword.
             Use 'ipv6 ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr.**(p. 577)**
- **address** -- Set IPv6 parameters for communication within an IP network**(p. 574)**

ipv6-addr

- [no] svlan *VLAN-ID* ipv6 address *IPV6-ADDR*

```
Configure a link-local IPv6 address.
```

Next Available Option:

- **link-local** -- Configure a link-local IPv6 address.**(p. 580)**

ipv6-addr/mask

- [no] svlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN*

```
Configure IPv6 address represented in CIDR notation.
```

Next Available Options:

- **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes**(p. 576)**
- **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface**(p. 578)**

jumbo

- [no] svlan *VLAN-ID* jumbo

```
Usage: [no] jumbo

Description: Labels this VLAN as a Jumbo VLAN, allowing you to pass
             packets up to 9220 bytes in size.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

link-local

- [no] svlan *VLAN-ID* ipv6 address *IPV6-ADDR* link-local

```
Configure a link-local IPv6 address.
```

mirror

- svlan *VLAN-ID* monitor all < *In* | *Out* | *Both* > mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 581)**
- **mirror_session_name** -- Mirror destination name.**(p. 580)**

- svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* < *In* > mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 581)**
- **mirror_session_name** -- Mirror destination name.**(p. 580)**

mirror_session_name

- [no] svlan *VLAN-ID* monitor all < *In* | *Out* | *Both* > mirror

```
Mirror destination name.
```

- [no] svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* < *In* > mirror

```
Mirror destination name.
```

monitor

- [no] svlan *VLAN-ID* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
              [1-4 | NAME-STR]...
       2) [no] monitor ip access-group <ACL-NAME> <in> mirror
              <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the VLAN is to be monitored or not.
             The network traffic seen by the monitored VLAN is copied to
             the Mirroring Destination to which a network analyzer can be
             attached.
             Note: When mirroring a VLAN in a busy network,
             some frames may not be copied to the mirroring port.
             This is an VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID command.

Parameters:  o 1-4 - Mirror destination number
             o NAME-STR - Friendly name associated with the mirror
             destination number.
             o ACL-NAME - Standard or Extended Access Control List number.
             o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 576)**
- **ip** -- Apply an IPv4 access list.**(p. 578)**

monitor_mirror_ACL_dir

- svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 580)**

monitor_mirror_session_id

- [no] svlan *VLAN-ID* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

  ```
  Mirror destination number.
  ```

  Range: < 1 to 4 >
- [no] svlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

  ```
  Mirror destination number.
  ```

  Range: < 1 to 4 >

name

- svlan *VLAN-ID* name *NAME*

```
Usage: name ASCII-STR

Description: Set the VLAN's name.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

priority

- svlan *VLAN-ID* qos priority *< 0 | 1 | 2 | ... >*

```
Specify priority to use.
```

Supported Values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

protocol

- svlan *VLAN-ID* protocol

```
Set a predefined protocol for the current VLAN.
```

Next Available Options:

- **protocols** < IPX | IPv4 | IPv6 | ... > -- Set a predefined protocol for the current VLAN. **(p. 582)**
- **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 582)**

protocol-group

- [no] svlan *VLAN-ID* protocol *PROTOCOL-GROUP*

```
Enter a list of protocols for the current VLAN delimited by commas.
```

protocols

- [no] svlan *VLAN-ID* protocol *< IPX | IPv4 | IPv6 | ... >*

```
Set a predefined protocol for the current VLAN.
```

Supported Values:

- **IPX** -- IPX Protocol Group
- **IPv4** -- IP version 4 Protocol Group
- **IPv6** -- IP version 6 Protocol Group
- **ARP** -- Address Resolution Protocol Group
- **Appletalk** -- Appletalk Protocol Group
- **SNA** -- System Network Architecture Protocol Group
- **NetBEUI** -- Network BIOS Enhanced User Interface Protocol Group

qos

- [no] svlan *VLAN-ID* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]

Description: Set VLAN-based priority. The 'dscp' or 'priority' must
             be specified if 'no' is not used. Using 'no' configures
             the switch not to apply a VLAN priority override to this
             VLAN's packets.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 577)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 581)**

rapid-commit

- [no] svlan *VLAN-ID* ipv6 address dhcp full rapid-commit

```
Obtain IPv6 address quickly from DHCPv6 server.
```

src-ip

- svlan *VLAN-ID* connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

tagged

- [no] svlan *VLAN-ID* tagged *[ETHERNET] PORT-LIST*

```
Usage: [no] tagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as tagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

unblock

- svlan *VLAN-ID* connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 576)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 578)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 583)**

untagged

- [no] svlan *VLAN-ID* untagged *[ETHERNET] PORT-LIST*

```
Usage: [no] untagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as untagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

voice

- [no] svlan *VLAN-ID* voice

```
Usage: [no] voice

Description: Labels this VLAN as a Voice VLAN, allowing you to separate,
             prioritize, and authenticate voice traffic moving through
```

```
your network.
This is a VLAN context command. It can be called directly
from the VLAN context or follow the 'vlan VLAN-ID'
command.
```

tacacs-server

OVERVIEW

Category:	Accounting
Primary context:	config
Related Commands	**show tacacs (page 513)**

```
Usage:  [no] tacacs-server host IP-ADDR [key KEY-STR]
        [no] tacacs-server key KEY-STR
             tacacs-server timeout <1-255>

Description: Configure TACACS+ authentication servers.
             The first version of the command adds (or removes, if 'no' is
             specified) a TACACS+ server to (from) the list of servers that
             will be used for authentication. Up to 3 TACACS+ servers can be
             configured. If 'key' is specified then this command also sets
             (or removes) an encryption key used during the authentication
             session with given server.
             The second version sets (or removes, with 'no') the global
             encryption key for TACACS+ authentication.
             The last version sets the response timeout interval for
             TACACS+ server.

Parameters:

    o address IP-ADDR [key KEY-STR] - Specifies the IP address of the
             server to use. Optional parameter 'key KEY-STR' specifies
             an encryption key used during the authentication session with
             given server. Specifying this key overrides the key set by
             the global configuration 'tacacs-server key KEY-STR' command
             for this server only.
    o key KEY-STR - Up to 100 characters. Encryption key used for TACACS+
             authentication. Default value is null, which means TACACS+
             packets are sent using clear text. The KEY-STR parameter is
             not allowed when a key is removed.
    o timeout <1-255> - Sets the timeout interval in seconds the TACACS+
             server must send response back to the switch.
             If this interval expires and no response the next configured
             server is queried. Default value is 5 seconds.
```

COMMAND STRUCTURE

- [no] tacacs-server **host** -- IP address of the server to use. (IP-ADDR) **(p. 586)**
  - **key** -- Encryption key to use with server. **(p. 586)**
    - **key** -- (ASCII-STR) **(p. 586)**
- [no] tacacs-server **key** -- Global encryption key. **(p. 586)**
  - **key** -- (ASCII-STR) **(p. 586)**
- tacacs-server **timeout** **< 1 to 255 >** -- Server timeout interval. **(p. 587)**

EXAMPLES

Example: tacacs-server host

Delete a per-server encryption key in the switch, and re-enter the 'tacacs-server host' command without the key parameter. For example, if you have north01 configured as the encryption key for a TACACS+ server with an IP address of 10.28.227.104 and you want to eliminate the key, use this command:

```
ProCurve(config)# tacacs-server host 10.28.227.104
```

Example: tacacs-server host key

Configure north01 as a per-server encryption key:

```
ProCurve(config)# tacacs-server host 10.28.227.63 key north01
```

Example: tacacs-server key

Configure north01 as a global encryption key:

```
ProCurve(config) tacacs-server key north01
```

Example: tacacs-server timeout

Change the timeout period from 5 seconds (the default) to 3 seconds:

```
HPswitch(config)# tacacs-server timeout 3
```

COMMAND DETAILS

host (p. 586)	**key (p. 586)**	**timeout (p. 587)**

host

- [no] tacacs-server host *IP-ADDR*

  IP address of the server to use.

  Next Available Option:
  - **key** -- Encryption key to use with server.**(p. 586)**

key

- [no] tacacs-server host *IP-ADDR* key

  Encryption key to use with server.

  Next Available Option:
  - **key** -- (ASCII-STR) **(p. 586)**

- tacacs-server host *IP-ADDR* key *KEY*

- [no] tacacs-server key

  Global encryption key.

Next Available Option:

- **key** -- (ASCII-STR) **(p. 586)**

- tacacs-server key *KEY*

timeout

- tacacs-server timeout *< 1 to 255 >*

```
Server timeout interval.
```

Range: < 1 to 255 >

telnet

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	

```
Usage: telnet <IPV4-ADDR|IPV6-ADDR|SWITCH-NUM>

Description: Initiate an outbound telnet session to another network device.
             The destination can be specified using one of the following
             parameter types:

    o IPV4-ADDR - IPv4 address of device to telnet to.
    o IPV6-ADDR - IPv6 address of device to telnet to.
    o SWITCH-NUM - The stack member number to telnet to. (1..16)
                   This parameter can only be used if stacking is enabled,
                   and this switch is acting as a commander.
```

COMMAND STRUCTURE

- telnet **ipv4-addr** -- IPv4 address of the device to telnet to. (IP-ADDR) **(p. 588)**
- telnet **ipv6-addr** -- IPv6 address of the device to connect to. (IPV6-ADDR) **(p. 588)**
- telnet **SWITCH-NUM** -- The stack member number to which to telnet. (NUMBER) **(p. 588)**

EXAMPLES

Example: telnet IP-ADDR

Establish a Telnet session with the device at IP address 10.0.0.2:

```
ProCurve(config)# telnet 10.0.0.2
```

COMMAND DETAILS

ipv4-addr (p. 588)	**ipv6-addr (p. 588)**	**SWITCH-NUM (p. 588)**

ipv4-addr

- telnet *IP-ADDR*

```
IPv4 address of the device to telnet to.
```

ipv6-addr

- telnet *IPV6-ADDR*

```
IPv6 address of the device to connect to.
```

SWITCH-NUM

- telnet *NUMBER*

```
The stack member number to which to telnet.
```

telnet6-server

OVERVIEW

Category:	
Primary context:	config
Related Commands	**telnet-server (page 590)** **show console (page 465)**

```
Usage: [no] telnet6-server

Description: Use at the global config level to enable/disable the IPv6
             telnet server on the switch.
             For remote clients to use telnet, the switch must first be
             configured for IPv6. By default, telnet access is enabled.
             Use 'show console' command to see the status of this function.
```

NOTES

Disabling Telnet Access

To disable inbound Telnet access completely, you must disable Telnet access

for both IPv6 and IPv4. The command for disabling Telnet4 access is

"no telnet-server".

To disable IPv6 Telnet access the command is "no telnet6-server".

COMMAND STRUCTURE

telnet-server

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show console (page 465)**

```
Usage: [no] telnet-server

Description: Enable/disable the IPv4 telnet server on the switch.
             For remote clients to use telnet, the switch must first be
             configured for IPv4. By default, telnet access is enabled.
             Use 'show console' command to see the status of this function.
```

COMMAND STRUCTURE

EXAMPLES

Example: telnet-server

Re-enable inbound Telnet access:

```
ProCurve(config)# telnet-server
```

terminal

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show terminal (page 514)**

```
Usage: terminal [length <2-1000> | width <53-1920>]
```

```
Description: Set the dimensions of the terminal window.
```

COMMAND STRUCTURE

- terminal **length** **< 2 to 1000 >** -- Set the height of the terminal window (NUMBER) **(p. 591)**
- terminal **width** **< 61 to 1920 >** -- Set the width of the terminal window (NUMBER) **(p. 591)**

COMMAND DETAILS

length (p. 591)	**width (p. 591)**

length

- terminal length *< 2 to 1000 >*

  ```
  Usage: terminal length <2-1000>
  ```

  ```
  Description: Set the height of the terminal window.
  ```

  Range: < 2 to 1000 >

width

- terminal width *< 61 to 1920 >*

  ```
  Usage: terminal width <53-1920>
  ```

  ```
  Description: Set the width of the terminal window.
  ```

  Range: < 61 to 1920 >

tftp

OVERVIEW

Category:	
Primary context:	config
Related Commands	**tftp6 (page 593)**

```
Usage: [no] tftp [client|server]

Description: Enable/disable TFTP, trivial file transfer protocol.
If SFTP is enabled, TFTP will be disabled. If
SFTP is to be enabled using SNMP, both TFTP and
auto-TFTP MUST first be disabled.
```

COMMAND STRUCTURE

- [no] tftp **client** -- Enable/disable the IPv4 TFTP client **(p. 592)**
- [no] tftp **server** -- Enable/disable the IPv4 TFTP server **(p. 592)**

COMMAND DETAILS

client (p. 592)	**server (p. 592)**

client

- [no] tftp client

```
Enable/disable the IPv4 TFTP client
```

server

- [no] tftp server

```
Enable/disable the IPv4 TFTP server
```

tftp6

OVERVIEW

Category:	
Primary context:	config
Related Commands	tftp (page 592)

```
Usage: [no] tftp6 [client|server]

Description: Enable/disable TFTP6, trivial file transfer protocol.
             TFTP6 and auto-TFTP cannot be enabled if SFTP is
             already enabled. If SFTP is to be enabled,
             both TFTP and auto-TFTP MUST first be disabled.
             The TFTP6 client MUST be enabled for the "copy tftp"
             command to work with IPv6.
```

COMMAND STRUCTURE

- [no] tftp6 **client** -- Enable/disable the IPv6 TFTP client **(p. 593)**
- [no] tftp6 **server** -- Enable/disable the IPv6 TFTP server **(p. 593)**

COMMAND DETAILS

client (p. 593)	server (p. 593)

client

- [no] tftp6 client

```
Enable/disable the IPv6 TFTP client
```

Default: Enabled

server

- [no] tftp6 server

```
Enable/disable the IPv6 TFTP server
```

Default: Enabled

time

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**ip (page 269)** **sntp (page 547)** **clock (page 76)**

```
Usage: time [HH:MM:SS] [MM/DD[/[yy]yy]]
            [daylight-time-rule <none|alaska|continental-us-and-canada|
                                 middle-europe-and-portugal|
                                 southern-hemisphere|
                                 western-europe|user-defined>
                                 [begin-date <MM/DD>] [end-date <MM/DD>]
            [timezone <-720..840>]

Description: Display/set current time, date, and local time parameters.
             Called without any parameters displays the information
             mentioned above.

Parameters:
    o HH:MM:SS           - New time.
    o MM/DD[/[yy]yy]     - New date.
    o timezone           - The number of minutes your location is to the
                           West(-) or East(+) of GMT. Default is 0.
    o daylight-time-rule - The daylight savings time rule for your location.
                           'none' (default) disables daylight savings time.
                           'begin-date' and 'end-date' are valid only if the
                           daylight time rule is set to 'user-defined'.
    o begin-date         - Set the beginning date for daylight savings time.
    o end-date           - Set the ending dates for daylight savings time.
                           Daylight savings time adjustment will be made at
                           2:00 AM on the first Sunday on or after the
                           specified date.
```

COMMAND STRUCTURE

- time **begin-date** -- The begin date of daylight savings time (MM/DD) **(p. 595)**
- time **date** -- New date (MM/DD[/[YY]YY]) **(p. 595)**
- time **daylight-time-rule < None | Alaska | Continental-US-and-Canada | ... >** -- The daylight savings time rule for your location **(p. 595)**
- time **end-date** -- The end date of daylight savings time (MM/DD) **(p. 595)**
- time **time** -- New time (HH:MM[:SS]) **(p. 595)**
- time **timezone < -720 to 840 >** -- The number of minutes your location is West(-) or East(+) of GMT **(p. 595)**

EXAMPLES

Example: time MM/DD[/[YY]YY]

Set the time on the switch to 9:45 a.m. on November 17, 2002:

```
ProCurve(config)# time 9:45 11/17/02
```

Example: timesync sntp

Select SNTP as the time source and configure it with unicast mode and an SNTP server at 10.28.227.141 with the default server version (3) and default poll interval (720 seconds):

```
ProCurve(config)# timesync sntp
```

Example: time timezone daylight-time-rule

Set the time zone and daylight time rule for Vancouver, Canada:

```
ProCurve(config)# time timezone -480 daylight-time-rule continental-us-and-canada
```

COMMAND DETAILS

begin-date

- time begin-date *MM/DD*

  ```
  The begin date of daylight savings time
  ```

date

- time *[DATE]*

  ```
  New date
  ```

daylight-time-rule

- time daylight-time-rule *< None | Alaska | Continental-US-and-Canada | ... >*

  ```
  The daylight savings time rule for your location
  ```

  Supported Values:
  - **None**
  - **Alaska**
  - **Continental-US-and-Canada**
  - **Middle-Europe-and-Portugal**
  - **Southern-Hemisphere**
  - **Western-Europe**
  - **User-defined**

end-date

- time end-date *MM/DD*

  ```
  The end date of daylight savings time
  ```

time

- time *[TIME]*

  ```
  New time
  ```

timezone

- time timezone *< -720 to 840 >*

```
The number of minutes your location is West(-) or East(+) of GMT
```

Range: < -720 to 840 >

timesync

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**ip (page 269)** **sntp (page 547)** **show timep (page 514)** **show sntp (page 508)**

```
Usage: [no] timesync <timep|sntp>
```

```
Description: Configure the network time protocol.
```

COMMAND STRUCTURE

- timesync **sntp** -- Set the time protocol to SNTP **(p. 597)**
- timesync **timep** -- Set the time protocol to the network time protocol **(p. 597)**

EXAMPLES

Example: timesync sntp

Select SNTP and configure it with unicast mode and an SNTP server at 10.28.227.141 with the default server version (3) and default poll interval (720 seconds):

```
ProCurve(config)# timesync sntp
ProCurve(config)# sntp unicast
ProCurve(config)# sntp server 10.28.227.141
```

COMMAND DETAILS

sntp (p. 597)	**timep (p. 597)**

sntp

- timesync sntp

```
Set the time protocol to SNTP
```

timep

- timesync timep

```
Set the time protocol to the network time protocol
```

traceroute

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	**ping (page 367)**

```
Usage: traceroute <IP-ADDR|hostname> [minttl <1-255>]
                  [maxttl <1-255>] [timeout <1-120>]
                  [probes <1-5>]

Description: Trace the IPv4 route to a device on the network.

Parameters:

   o IP-ADDR - IPv4 address of device to which to send traceroute.

   o hostname - Hostname of device to which to send IPv4 traceroute.

   o [minttl <1-255>] - Minimum number of hops used in outgoing probe
     packets. The default value is 1.

   o [maxttl <1-255>] - Maximum number of hops used in outgoing probe
     packets. The default value is 30.

   o [timeout <1-120>] - Time (in seconds) to wait for a response to a
     probe. The default value is 5 seconds.

   o [probes <1-5>] - Number of probe queries to send out for each hop.
     The default value is 3.

Examples:

     (1) hp-switch# traceroute 1.1.1.1
```

COMMAND STRUCTURE

- traceroute **host-name** -- Hostname of the destination device. (ASCII-STR) **(p. 599)**
  - **maxttl < 1 to 255 >** -- Maximum time to live <1-255>. **(p. 599)**
  - **minttl < 1 to 255 >** -- Minimum time to live <1-255>. **(p. 599)**
  - **probes < 1 to 5 >** -- Number of Probes <1-5>. **(p. 600)**
  - **timeout < 1 to 120 >** -- Traceroute timeout in seconds <1-120>. **(p. 600)**
- traceroute **ip-addr** -- Destination IPv4 address. (IP-ADDR) **(p. 599)**
  - **maxttl < 1 to 255 >** -- Maximum time to live <1-255>. **(p. 599)**
  - **minttl < 1 to 255 >** -- Minimum time to live <1-255>. **(p. 599)**
  - **probes < 1 to 5 >** -- Number of Probes <1-5>. **(p. 600)**
  - **timeout < 1 to 120 >** -- Traceroute timeout in seconds <1-120>. **(p. 600)**

EXAMPLES

Example: traceroute IP-ADDR

Trace the route to the device that has IP address 10.168.1.146:

```
ProCurve# traceroute 10.168.1.146
traceroute to 10.168.1.146 ,
              1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.57.191.129         2 ms       3 ms       3 ms
 2 10.57.232.1           4 ms       2 ms       3 ms
 3 10.168.1.146          4 ms       3 ms       3 ms
```

COMMAND DETAILS

host-name (p. 599)	**maxttl (p. 599)**	**probes (p. 600)**
ip-addr (p. 599)	**minttl (p. 599)**	**timeout (p. 600)**

host-name

- traceroute *HOST-NAME*

  ```
  Hostname of the destination device.
  ```

  Next Available Options:
  - **minttl** < 1 to 255 > -- Minimum time to live <1-255>.**(p. 599)**
  - **maxttl** < 1 to 255 > -- Maximum time to live <1-255>.**(p. 599)**
  - **timeout** < 1 to 120 > -- Traceroute timeout in seconds <1-120>.**(p. 600)**
  - **probes** < 1 to 5 > -- Number of Probes <1-5>.**(p. 600)**

ip-addr

- traceroute *IP-ADDR*

  ```
  Destination IPv4 address.
  ```

  Next Available Options:
  - **minttl** < 1 to 255 > -- Minimum time to live <1-255>.**(p. 599)**
  - **maxttl** < 1 to 255 > -- Maximum time to live <1-255>.**(p. 599)**
  - **timeout** < 1 to 120 > -- Traceroute timeout in seconds <1-120>.**(p. 600)**
  - **probes** < 1 to 5 > -- Number of Probes <1-5>.**(p. 600)**

maxttl

- traceroute *IP-ADDR* maxttl *< 1 to 255 >*

  ```
  Maximum time to live <1-255>.
  ```

  Range: < 1 to 255 >
- traceroute *HOST-NAME* maxttl *< 1 to 255 >*

  ```
  Maximum time to live <1-255>.
  ```

  Range: < 1 to 255 >

minttl

- traceroute *IP-ADDR* minttl *< 1 to 255 >*

  ```
  Minimum time to live <1-255>.
  ```

  Range: < 1 to 255 >
- traceroute *HOST-NAME* minttl *< 1 to 255 >*

```
Minimum time to live <1-255>.
```

Range: < 1 to 255 >

probes

- traceroute *IP-ADDR* probes *< 1 to 5 >*

  ```
  Number of Probes <1-5>.
  ```

  Range: < 1 to 5 >
- traceroute *HOST-NAME* probes *< 1 to 5 >*

  ```
  Number of Probes <1-5>.
  ```

  Range: < 1 to 5 >

timeout

- traceroute *IP-ADDR* timeout *< 1 to 120 >*

  ```
  Traceroute timeout in seconds <1-120>.
  ```

  Range: < 1 to 120 >
- traceroute *HOST-NAME* timeout *< 1 to 120 >*

  ```
  Traceroute timeout in seconds <1-120>.
  ```

  Range: < 1 to 120 >

traceroute6

OVERVIEW

Category:	
Primary context:	operator
Related Commands	**ping (page 367)** **traceroute (page 598)** **ping6 (page 369)**

```
Usage: traceroute6 <IPV6-ADDR|hostname> [minttl <1-255>]
                  [maxttl <1-255>] [timeout <1-120>]
                  [probes <1-5>]

Description: Trace the IPv6 route to a device on the network.

Parameters:

   o IPV6-ADDR - IPv6 address of device to which to send traceroute.

   o hostname - Hostname of deivce to which to send IPv6 traceroute.

   o [minttl <1-255>] - Minimum number of hops used in outgoing probe
     packets. The default value is 1.

   o [maxttl <1-255>] - Maximum number of hops used in outgoing probe
     packets. The default value is 30.

   o [timeout <1-120>] - Time (in seconds) to wait for a response to a
     probe. The default value is 5 seconds.

   o [probes <1-5>] - Number of probe queries to send out for each hop.
     The default value is 3.

Examples:

(1) hp-switch# traceroutev6 80fe::20b:cdff:fedd:9a62

(2)ProCurve# traceroute6 2001:db8::10

 traceroute to 2001:db8::10
                  1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1  2001:db8::a:1c:e3:3           0 ms    0 ms    0 ms
 2  2001:db8:0:7::5               7 ms    3 ms    0 ms
 3  2001:db8::214:c2ff:fe4c:e480  0 ms    1 ms    0 ms
 4  2001:db8::10                  0 ms    1 ms    0 ms
```

COMMAND STRUCTURE

- traceroute6 **host-name** -- Hostname of the destination device. (ASCII-STR) **(p. 602)**
  - **maxttl < 1 to 255 >** -- Maximum time to live <1-255>. **(p. 602)**
  - **minttl < 1 to 255 >** -- Minimum time to live <1-255>. **(p. 603)**
  - **probes < 1 to 5 >** -- Number of Probes <1-5>. **(p. 603)**
  - **timeout < 1 to 120 >** -- Traceroute timeout in seconds <1-120>. **(p. 603)**

- traceroute6 **ipv6-addr** -- Destination IPv6 adddress. (IPV6-ADDR) **(p. 602)**
  - **maxttl < 1 to 255 >** -- Maximum time to live <1-255>. **(p. 602)**
  - **minttl < 1 to 255 >** -- Minimum time to live <1-255>. **(p. 603)**
  - **probes < 1 to 5 >** -- Number of Probes <1-5>. **(p. 603)**
  - **timeout < 1 to 120 >** -- Traceroute timeout in seconds <1-120>. **(p. 603)**

COMMAND DETAILS

host-name (p. 602)	**maxttl (p. 602)**	**probes (p. 603)**
ipv6-addr (p. 602)	**minttl (p. 603)**	**timeout (p. 603)**

host-name

- traceroute6 *HOST-NAME*

```
Hostname of the destination device.
```

Next Available Options:

- **minttl** < 1 to 255 > -- Minimum time to live <1-255>.**(p. 603)**
- **maxttl** < 1 to 255 > -- Maximum time to live <1-255>.**(p. 602)**
- **timeout** < 1 to 120 > -- Traceroute timeout in seconds <1-120>.**(p. 603)**
- **probes** < 1 to 5 > -- Number of Probes <1-5>.**(p. 603)**

ipv6-addr

- traceroute6 *IPV6-ADDR*

```
Destination IPv6 adddress.
```

Next Available Options:

- **minttl** < 1 to 255 > -- Minimum time to live <1-255>.**(p. 603)**
- **maxttl** < 1 to 255 > -- Maximum time to live <1-255>.**(p. 602)**
- **timeout** < 1 to 120 > -- Traceroute timeout in seconds <1-120>.**(p. 603)**
- **probes** < 1 to 5 > -- Number of Probes <1-5>.**(p. 603)**

maxttl

- traceroute6 *IPV6-ADDR* maxttl *< 1 to 255 >*

```
Maximum number of hops allowed for each probe packet sent along the
route. If the maxttl value is less than the actual number of hops
required to reach the host, the traceroute output displays only the
IPv6 addresses of the hops detected by the configured maxttl value. <1-255>.
```

Range: < 1 to 255 >

Default: 30

- traceroute6 *HOST-NAME* maxttl *< 1 to 255 >*

```
Maximum number of hops allowed for each probe packet sent along the
route. If the maxttl value is less than the actual number of hops
required to reach the host, the traceroute output displays only the
IPv6 addresses of the hops detected by the configured maxttl value. <1-255>.
```

Range: < 1 to 255 >

Default: 30

minttl

- traceroute6 *IPV6-ADDR* minttl *< 1 to 255 >*

```
Minimum number of hops allowed for each probe packet sent along the
route. If the minttl value is greater than the actual number of hops,
the traceroute output displays only the hops equal to or greater than the
configured minttl threshold value.
If the minttl value is the same as the actual number of hops, only
the final hop is displayed in the command output.
If the minttl value is less than the actual number of hops, all hops
to the destination host are displayed. <1-255>.
```

Range: < 1 to 255 >

Default: 1

- traceroute6 *HOST-NAME* minttl *< 1 to 255 >*

```
Minimum number of hops allowed for each probe packet sent along the
route. If the minttl value is greater than the actual number of hops,
the traceroute output displays only the hops equal to or greater than the
configured minttl threshold value.
If the minttl value is the same as the actual number of hops, only
the final hop is displayed in the command output.
If the minttl value is less than the actual number of hops, all hops
to the destination host are displayed. <1-255>.
```

Range: < 1 to 255 >

Default: 1

probes

- traceroute6 *IPV6-ADDR* probes *< 1 to 5 >*

```
Number of times a traceroute is performed to locate the IPv6 device
at any hop in the route to the specified host before the operation
times out. <1-5>.
```

Range: < 1 to 5 >

Default: 3

- traceroute6 *HOST-NAME* probes *< 1 to 5 >*

```
Number of times a traceroute is performed to locate the IPv6 device
at any hop in the route to the specified host before the operation
times out. <1-5>.
```

Range: < 1 to 5 >

Default: 3

timeout

- traceroute6 *IPV6-ADDR* timeout *< 1 to 120 >*

```
Number of seconds within which a response is required from the IPv6
device at each hop in the route to the destination host before the
traceroute operation times out. <1-120>.
```

Range: < 1 to 120 >

Default: 5 seconds

- traceroute6 *HOST-NAME* timeout *< 1 to 120 >*

  ```
  Number of seconds within which a response is required from the IPv6
  device at each hop in the route to the destination host before the
  traceroute operation times out. <1-120>.
  ```

  Range: < 1 to 120 >

  Default: 5 seconds

trunk

OVERVIEW

Category:	Traffic Management
Primary context:	config
Related Commands	**show trunks (page 515)**

```
Usage: trunk [ethernet] PORT-LIST
             <trk1|trk2...trkN>
             [trunk|lacp]
       no trunk [ethernet] PORT-LIST

Description: Add or remove a switch port from a port trunk.
             Each port on the switch (up to 8 ports total) can be made
             a member of a port trunk. The 'no trunk' command can be used
             to remove ports from an existing trunk. The switch supports
             any one of the following trunk groups:

             Trunk - A static port grouping in which no protocols are used
             to create or maintain the trunk (type 'trunk').

             LACP - A port groping in which trunk membership is dynamically
             determined using the IEEE 802.1ad Link Aggregation Protocol.
             For LACP trunks the trunk group may instead be manually
             configured as static trunk.
             Manually configuring a static LACP trunk allows you to specify
             which ports are members and still configure advanced LACP
             features (type 'lacp').

             Any trunk group can have up to 8 member ports. All ports that
             belong to the same trunk group must have the same port type.
             All trunk groups use an algorithm that considers the source and
             destination MAC addresses for load distribution.

             General Considerations: To avoid broadcast storms, or
             loops in your network while configuring trunks, first
             disable or disconnect all the ports you wish to add or
             remove from both sides of the trunk.  Once done configuring
             the trunk, enable or re-connect the ports.
```

COMMAND STRUCTURE

- trunk **portlist** -- Specify the ports that are to be added to/removed from a trunk. ([ethernet] PORT-LIST) **(p. 606)**
  - **trunk-group < Trk1 | Trk2 | Trk3 | ... >** -- Specify the trunk group a port is to be a member of. **(p. 606)**
    - **type < Trunk | LACP | | ... >** -- Specify protocol to use on a manually configured trunk. **(p. 607)**

EXAMPLES

Example: trunk

Use ports C4 - C6 to create a non-protocol static trunk group with the group name of trk2:

```
ProCurve(config)# trunk c4-c6 trk2 trunk
```

COMMAND DETAILS

portlist

- trunk *[ETHERNET] PORT-LIST*

  `Specify the ports that are to be added to/removed from a trunk.`

  Next Available Option:

  - **trunk-group** < Trk1 | Trk2 | Trk3 | ... > -- Specify the trunk group a port is to be a member of. **(p. 606)**

trunk-group

- trunk *[ETHERNET] PORT-LIST < Trk1 | Trk2 | Trk3 | ... >*

  `Specify the trunk group a port is to be a member of.`

  Supported Values:

  - **Trk1** -- Trunk group 1
  - **Trk2** -- Trunk group 2
  - **Trk3** -- Trunk group 3
  - **Trk4** -- Trunk group 4
  - **Trk5** -- Trunk group 5
  - **Trk6** -- Trunk group 6
  - **Trk7** -- Trunk group 7
  - **Trk8** -- Trunk group 8
  - **Trk9** -- Trunk group 9
  - **Trk10** -- Trunk group 10
  - **Trk11** -- Trunk group 11
  - **Trk12** -- Trunk group 12
  - **Trk13** -- Trunk group 13
  - **Trk14** -- Trunk group 14
  - **Trk15** -- Trunk group 15
  - **Trk16** -- Trunk group 16
  - **Trk17** -- Trunk group 17
  - **Trk18** -- Trunk group 18
  - **Trk19** -- Trunk group 19
  - **Trk20** -- Trunk group 20
  - **Trk21** -- Trunk group 21
  - **Trk22** -- Trunk group 22
  - **Trk23** -- Trunk group 23
  - **Trk24** -- Trunk group 24
  - **Trk25** -- Trunk group 25
  - **Trk26** -- Trunk group 26
  - **Trk27** -- Trunk group 27
  - **Trk28** -- Trunk group 28
  - **Trk29** -- Trunk group 29
  - **Trk30** -- Trunk group 30
  - **Trk31** -- Trunk group 31

- **Trk32** -- Trunk group 32
- **Trk33** -- Trunk group 33
- **Trk34** -- Trunk group 34
- **Trk35** -- Trunk group 35
- **Trk36** -- Trunk group 36
- **Trk37** -- Trunk group 37
- **Trk38** -- Trunk group 38
- **Trk39** -- Trunk group 39
- **Trk40** -- Trunk group 40
- **Trk41** -- Trunk group 41
- **Trk42** -- Trunk group 42
- **Trk43** -- Trunk group 43
- **Trk44** -- Trunk group 44
- **Trk45** -- Trunk group 45
- **Trk46** -- Trunk group 46
- **Trk47** -- Trunk group 47
- **Trk48** -- Trunk group 48
- **Trk49** -- Trunk group 49
- **Trk50** -- Trunk group 50
- **Trk51** -- Trunk group 51
- **Trk52** -- Trunk group 52
- **Trk53** -- Trunk group 53
- **Trk54** -- Trunk group 54
- **Trk55** -- Trunk group 55
- **Trk56** -- Trunk group 56
- **Trk57** -- Trunk group 57
- **Trk58** -- Trunk group 58
- **Trk59** -- Trunk group 59
- **Trk60** -- Trunk group 60

Next Available Option:

- **type** < Trunk | LACP | | ... > -- Specify protocol to use on a manually configured trunk. **(p. 607)**

type

- trunk *[ETHERNET] PORT-LIST < Trk1 | Trk2 | Trk3 | ... > < Trunk | LACP | | ... >*

```
Specify protocol to use on a manually configured trunk.
```

Supported Values:

- **Trunk** -- Do not use any protocol to create or maintain the trunk.
- **LACP** -- Use IEEE 802.1ad Link Aggregation protocol.

update

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	

```
Usage: update
```

```
Description: Enter Monitor ROM Console.
```

COMMAND STRUCTURE

upgrade-software

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: upgrade-software SOFTWARE-KEY

Description: Enter a key to upgrade system software and enable advanced
             features.
```

COMMAND STRUCTURE

virus-throttle

OVERVIEW

Category:	Troubleshooting
Primary context:	config
Related Commands	**connection-rate-filter (page 80)**

```
Usage:       [no] virus-throttle

Description: To configure virus throttling, please use the
             'connection-rate-filter' command.
```

COMMAND STRUCTURE

vlan

OVERVIEW

Category:	VLANs
Primary context:	config
Related Commands	**show vlans (page 521)** **ip (page 269)** **ipv6 (page 291)** **router (page 407)** **mirror-port (page 358)**

```
Usage: [no] vlan VLAN-ID [...]

Description: Add, delete, edit VLAN configuration or enter a VLAN context.
             If an existing VLAN-ID is specified you are put into the
             context for that VLAN, and can then execute commands for that
             VLAN. If a new VLAN-ID is specified, the new VLAN is added with
             the VLAN-ID, and you are put into the context of the new VLAN.
             If you follow the command with one of the VLAN Context commands
             in the same command line, the context level is not changed, but
             the commands are executed for the VLAN specified by the
             VLAN-ID. The 'no' option of the VLAN command is used to delete
             the VLAN specified by VLAN-ID.
```

COMMAND STRUCTURE

- vlan VLAN-ID **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 625)**
- vlan VLAN-ID **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter **(p. 626)**
  - **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 653)**
    - **all** -- Resets all previously blocked by the connection rate filter **(p. 621)**
    - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 631)**
    - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 651)**
- [no] vlan VLAN-ID **dhcp-snooping** -- **(p. 627)**
- [no] vlan VLAN-ID **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 629)**
- [no] vlan VLAN-ID **igmp-proxy** -- Associate an IGMP proxy domain with a VLAN **(p. 632)**
  - **domain-name < END OF PRINTABLE >** -- Specify the domain name to associate/disassociate with the VLAN. (ASCII-STR) **(p. 627)**
- [no] vlan VLAN-ID **ip** -- Configure various IP parameters for the VLAN **(p. 633)**
  - **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 618)**
    - **direction < in | out | connection-rate-filter | ... >** -- **(p. 627)**
  - **address** -- Set IP parameters for communication within an IP network **(p. 619)**
    - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 627)**
    - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 633)**
  - **forward-protocol** -- Add or remove a UDP server address for the VLAN **(p. 629)**
    - **udp** -- Add or remove a UDP server address for the VLAN **(p. 652)**
      - **ip-addr** -- IP address of the protocol server. (IP-ADDR) **(p. 633)**
        - **port-name < dns | ntp | netbios-ns | ... >** -- (NUMBER) **(p. 645)**

      - **port-num** -- UDP port number of the server. (TCP/UDP-PORT) **(p. 645)**
- **helper-address** -- Add or remove a DHCP server IP address for the VLAN (IP-ADDR) **(p. 631)**
- **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature on a VLAN **(p. 632)**
  - **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 625)**
  - **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 625)**
  - **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 628)**
  - **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 629)**
  - **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 629)**
  - **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups **(p. 631)**
  - **querier** -- Specify querier/non-querier capability for the VLAN **(p. 648)**
    - **interval < 5 to 300 >** -- Sets the interval in seconds between IGMP queries (default: 125) **(p. 632)**
- **irdp** -- Configure ICMP Router Discovery Protocol (IRDP) **(p. 636)**
  - **advert-address < multicast | broadcast >** -- Specify the destination address to be used for router advertisements **(p. 620)**
  - **holdtime < 4 to 9000 >** -- Set the lifetime (in seconds) of the router advertisements sent on this interface **(p. 631)**
  - **maxadvertinterval < 4 to 1800 >** -- Set the maximum time (in seconds) allowed between sending unsolicited router advertisements **(p. 638)**
  - **minadvertinterval < 3 to 1800 >** -- Set the minimum time (in seconds) allowed between sending unsolicited router advertisements **(p. 639)**
  - **preference** -- The preferability of the router as a default router, relative to the other routers on the same subnet **(p. 646)**
    - **no-default** -- Indicates that the router should never be used as a default by its neighbors. **(p. 642)**
    - **number < -2147483647 to 2147483647 >** -- The router preferability number. Higher values are more preferable. **(p. 642)**
- **local-proxy-arp** -- Enable/disable local proxy ARP **(p. 637)**
- **mroute** -- Configure IP Multicast Routing parameters on the VLAN interface **(p. 641)**
  - **ttl-threshold < 0 to 255 >** -- Set the multicast datagram TTL threshold for the interface **(p. 652)**
- **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the VLAN interface **(p. 642)**
  - **all** -- Process the request for all IP addresses. **(p. 621)**
    - **area** -- Specify an OSPF area. **(p. 622)**
      - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 622)**
      - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 625)**
    - **authentication** -- Disable authentication. **(p. 623)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 623)**
      - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 623)**
    - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 626)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 627)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 630)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 638)**
      - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 626)**
    - **passive** -- Configures an ospf interface as passive. **(p. 643)**
    - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 646)**

    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 649)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 652)**
  - **area** -- Specify an OSPF area. **(p. 622)**
    - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 622)**
    - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 625)**
  - **authentication** -- Disable authentication. **(p. 623)**
  - **authentication-key** -- Set simple authentication method and key. **(p. 623)**
    - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 623)**
  - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 626)**
  - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 627)**
  - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 630)**
  - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 633)**
    - **area** -- Specify an OSPF area. **(p. 622)**
      - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 622)**
      - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 625)**
    - **authentication** -- Disable authentication. **(p. 623)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 623)**
      - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 623)**
    - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 626)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 627)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 630)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 638)**
      - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 626)**
    - **passive** -- Configures an ospf interface as passive. **(p. 643)**
    - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 646)**
    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 649)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 652)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 638)**
    - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 626)**
  - **passive** -- Configures an ospf interface as passive. **(p. 643)**
  - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 646)**
  - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 649)**
  - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 652)**
- **pim-dense** -- Enable/disable/configure PIM-DM protocol on the VLAN interface **(p. 643)**
  - **graft-retry-interval < 1 to 10 >** -- Set the interval a PIM router waits for a Graft Ack before resending a Graft on this interface **(p. 630)**
  - **hello-delay < 0 to 5 >** -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface **(p. 630)**
  - **hello-interval < 5 to 300 >** -- Set the frequency at which PIM Hello messages are transmitted on this interface **(p. 630)**
  - **ip-addr** -- Set the source IP address for the PIM-DM packets sent out on this interface **(p. 633)**
    - **any** -- Dynamically determine IP address. **(p. 622)**
    - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 633)**
  - **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface **(p. 637)**
  - **max-graft-retries < 1 to 10 >** -- Set the maximum number of times this router will resend a Graft on this interface **(p. 638)**

  - **override-interval < 500 to 6000 >** -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface **(p. 643)**
  - **propagation-delay < 250 to 2000 >** -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface **(p. 647)**
  - **ttl-threshold < 0 to 255 >** -- Set the Time To Live in a PIM-DM State Refresh message at which it is not forwarded on this interface **(p. 652)**
- **pim-sparse** -- Enable/disable/configure PIM-SM protocol on the VLAN interface **(p. 644)**
  - **dr-priority** -- Set the priority value to use on the interface in the Designated Router election process **(p. 627)**
  - **hello-delay < 0 to 5 >** -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface **(p. 630)**
  - **hello-interval < 5 to 300 >** -- Set the frequency at which PIM Hello messages are transmitted on this interface **(p. 630)**
  - **ip-addr** -- Set the source IP address for the PIM-SM packets sent out on this interface **(p. 633)**
    - **any** -- Dynamically determine IP address. **(p. 622)**
    - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 633)**
  - **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface **(p. 637)**
  - **nbr-timeout < 60 to 8000 >** -- Set the neighbour loss time interval for this interface **(p. 642)**
  - **override-interval < 500 to 6000 >** -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface **(p. 643)**
  - **propagation-delay < 250 to 2000 >** -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface **(p. 647)**
- **proxy-arp** -- Enable/disable proxy ARP **(p. 648)**
- **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the VLAN interface **(p. 650)**
  - **all** -- Process the request for all IP addresses. **(p. 621)**
    - **authentication-key** -- Set RIP authentication key (maximum 16 characters). **(p. 623)**
      - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 624)**
    - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 624)**
    - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 638)**
    - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 645)**
    - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 649)**
    - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 650)**
    - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 651)**
  - **authentication-key** -- Set RIP authentication key (maximum 16 characters). **(p. 623)**
    - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 624)**
  - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 624)**
  - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 633)**
    - **authentication-key** -- Set RIP authentication key (maximum 16 characters). **(p. 623)**
      - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 624)**
    - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 624)**
    - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 638)**
    - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 645)**
    - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 649)**

      - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 650)**
      - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 651)**
    - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 638)**
    - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 645)**
    - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 649)**
    - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 650)**
    - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 651)**
- [no] vlan VLAN-ID **ip-recv-mac-address** -- Associates a L3-mac-address with a VLAN **(p. 635)**
  - **mac-address** -- The L3-mac-address to be associated with a VLAN. (MAC-ADDR) **(p. 638)**
    - **interval** -- Specify the L3-Mac-Address timeout interval. **(p. 632)**
      - **timer-interval < 1 to 255 >** -- Timeout interval in seconds <1-255>. **(p. 652)**
- [no] vlan VLAN-ID **ipv6** -- Configure various IP parameters for the VLAN **(p. 635)**
  - **address** -- Set IPv6 parameters for communication within an IP network **(p. 619)**
    - **autoconfig** -- Automatic address configuration. **(p. 625)**
    - **dhcp** -- Configure a DHCPv6 client. **(p. 627)**
      - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server. **(p. 630)**
        - **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server. **(p. 649)**
    - **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 636)**
      - **link-local** -- Configure a link-local IPv6 address. **(p. 637)**
    - **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 636)**
      - **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes **(p. 622)**
      - **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface **(p. 628)**
  - **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr. **(p. 628)**
  - **mld** -- Enable/disable/configure IPv6 Multicast Listener Discovery (MLD) feature on a VLAN **(p. 639)**
    - **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 625)**
    - **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 625)**
    - **fastleave** -- Enables MLD fast-leaves on the specified ports in the selected VLAN ([ethernet] PORT-LIST) **(p. 628)**
    - **forcedfastleave** -- Enables MLD Forced Fast-Leave on the specified ports in the selected VLAN, even if they are cascaded ([ethernet] PORT-LIST) **(p. 629)**
    - **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 629)**
    - **querier** -- This command disables or re-enables the ability for the switch to become querier if necessary **(p. 648)**
- [no] vlan VLAN-ID **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size **(p. 637)**
- [no] vlan VLAN-ID **monitor** -- Define either the VLAN is to be monitored or not **(p. 640)**
  - **all < In | Out | Both >** -- Monitor all traffic. **(p. 621)**
    - **mirror** -- Mirror destination. **(p. 639)**
      - **mirror_session_name** -- Mirror destination name. **(p. 639)**
      - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 641)**

  - **ip** -- Apply an IPv4 access list. **(p. 633)**
    - **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 618)**
      - **monitor_mirror_ACL_dir < In >** -- Define the mirror port for diagnostic purposes **(p. 641)**
        - **mirror** -- Mirror destination. **(p. 639)**
          - **mirror_session_name** -- Mirror destination name. **(p. 639)**
          - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 641)**
- vlan VLAN-ID **name** -- Set the VLAN's name (ASCII-STR) **(p. 642)**
- [no] vlan VLAN-ID **protocol** -- Set a predefined protocol for the current VLAN. **(p. 647)**
  - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 647)**
  - **protocols < IPX | IPv4 | IPv6 | ... >** -- Set a predefined protocol for the current VLAN. **(p. 648)**
- [no] vlan VLAN-ID **qos** -- Set VLAN-based priority **(p. 648)**
  - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 628)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 646)**
- [no] vlan VLAN-ID **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 651)**
- [no] vlan VLAN-ID **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 653)**
- [no] vlan VLAN-ID **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network **(p. 653)**
- [no] vlan VLAN-ID **vrrp** -- Enable/disable/configure VRRP operation on the VLAN **(p. 654)**
  - **vrid < 1 to 255 >** -- Configure a virtual router instance for the VLAN **(p. 653)**
    - **advertise-interval < 1 to 255 >** -- Set time interval (in seconds) between sending VRRP advertisement messages **(p. 621)**
    - **backup** -- Designate the virtual router instance as a Backup **(p. 625)**
    - **enable** -- Enable/disable operation of the virtual router instance **(p. 628)**
    - **owner** -- Designate the virtual router instance as an Owner (Master) **(p. 643)**
    - **preempt-delay-time < 1 to 600 >** -- Enable the pre-emptive delay timer for the virtual router instance **(p. 645)**
    - **preempt-mode** -- Enable/disable preempt mode for the virtual router instance **(p. 646)**
    - **primary-ip-address** -- Specify IP address the virtual router instance will use as a source in VRRP advertisement messages **(p. 646)**
      - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 633)**
      - **lowest** -- Dynamically determine lowest IP address. **(p. 637)**
    - **priority < 1 to 255 >** -- Configure priority for the virtual router instance **(p. 646)**
    - **virtual-ip-address** -- Specify IP address to be supported by the virtual router instance **(p. 653)**
      - **ip-addr** -- Specify IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 633)**

EXAMPLES

Example: vlan name

Change VLAN 100's name to "Blue_Team" and add ports A1 - A5 as tagged members of the VLAN:

```
ProCurve(config)# vlan 100 name Blue_Team
ProCurve(config)# vlan 100 tagged a1-a5
```

Example: vlan default_vlan

Go to a different VLAN context level, such as to the default VLAN:

```
ProCurve(vlan-100)# vlan default_vlan
```

Example: vlan ip address

Configure IP addressing on the default VLAN with the subnet mask specified in mask bits:

```
ProCurve(config)# vlan 1 ip address 10.28.227.103 255.255.255.0
```

Example: vlan ip address

Configure the same IP addressing as the preceding example, but specify the subnet mask by mask length:

```
ProCurve(config)# vlan 1 ip address 10.28.227.103/24
```

Example: vlan ip address

Delete an IP address configured in VLAN 1:

```
ProCurve(config) no vlan 1 ip address 10.28.227.103/24
```

Example: vlan ip igmp

Configure IGMP on VLAN 1:

```
ProCurve(config)# vlan 1 ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
ProCurve(config)# ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
```

Example: vlan ip igmp high-priority-forward

Configure high priority for IGMP traffic on VLAN 1:

```
ProCurve(config)# vlan 1 ip igmp high-priority-forward
```

Example: vlan ip igmp high-priority-forward

Same as above command, but in the VLAN 1 context level:

```
ProCurve(vlan-1)# ip igmp high-priority-forward
```

Example: vlan ip igmp high-priority-forward

Return IGMP traffic to "normal" priority:

```
ProCurve(vlan 1)# no ip igmp high-priority-forward
```

Example: vlan tagged

Change the tagged ports in the above examples to No (or Auto, if GVRP is enabled):

```
ProCurve(config)# no vlan 100 tagged a1-a5
```

Example: vlan tagged

Configure a voice VLAN with a VID of 10, and set the highest priority for all traffic on this VLAN:

```
ProCurve(config)# vlan 10 qos priority 7
ProCurve(config)# write memory
```

COMMAND DETAILS

access-group

- [no] vlan *VLAN-ID* ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> <in|out>

in                     Match packets this device will route to another VLAN
out                    Match packets this device will route onto this VLAN
vlan                   Match packets that originate within this VLAN
connection-rate-filter Manage new conection rates originating in this VLAN

   Description: Apply the specified access control list on this VLAN interface.
                The ACL can match either packets that are routed from this VLAN
                to another VLAN, packets that will be routed from another VLAN
                to this VLAN, packets that originate on this VLAN, or it can
                manage new connection rates for virus throttling.
```

Next Available Option:

- **direction** < in | out | connection-rate-filter | ... > -- **(p. 627)**

- vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:

- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 641)**

address

- [no] vlan *VLAN-ID* ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.
             Each VLAN represents an IP interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ip address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:

    o dhcp-bootp - The switch attempts to get its configuration from a
      DHCP/Bootp server.

    o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch or VLAN.
      The IP-ADDR/MASK-LENGTH may be specified in two ways using the
      following syntax:
          ip address 192.32.36.87/24
          ip address 192.32.36.87 255.255.255.0
      Both of the statements above would have the same effect.
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 633)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 627)**

- [no] vlan *VLAN-ID* ipv6 address

```
Usage: [no] ipv6 address [dhcp|autoconfig|IPv6-ADDR/PREFIX-LEN]

Description: Set IPv6 parameters for communication within an IP network.
             Each VLAN represents an IPv6 interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ipv6 address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:
    o autoconfig - Enables automatic address configuration of IPv6
      addresses using stateless configuration of an interface .

    o dhcp - The switch attempts to get its configuration from a
      DHCPv6 server.

    o IPv6-ADDR/PREFIX-LEN-Assign an IPv6 address to the switch or VLAN.
      The IPv6-ADDR/PREFIX-LEN may be specified in four ways using the
      following syntax:
          ipv6 address 1234:abcd::5678/40
          ipv6 address 2001:0db8:1:1:ffff:ffff:ffff:fffe/64 anycast
          ipv6 address 2001:0db8:0:1::/64 eui-64
      Only link-local addreses are configured without PREFIX-LEN as below:
          ipv6 address FE80:0:0:0:0123:0456:0789:0abc link-local
      Multiple addresses may be configured on a single VLAN.
```

Next Available Options:

- **autoconfig** -- Automatic address configuration.**(p. 625)**
- **dhcp** -- Configure a DHCPv6 client.**(p. 627)**
- **ipv6-addr** -- Configure a link-local IPv6 address. (IPV6-ADDR) **(p. 636)**
- **ipv6-addr/mask** -- Configure IPv6 address represented in CIDR notation. (IPV6-ADDR/PREFIX-LEN) **(p. 636)**

advert-address

- vlan *VLAN-ID* ip irdp < *multicast* | *broadcast* >

```
Usage: [no] ip irdp <multicast|broadcast>

Description: Specify the destination address to be used for router
             advertisements.
             It has to be either multicast or broadcast. If the value
             of this object is 'multicast' (the default), router
             advertisements will be sent to the all-hosts multicast
             address, 224.0.0.1. If the value of this object is 'broadcast',
             router advertisements sent on this interface will be sent to
             the limitied broadcast address, 255.255.255.255.
```

Supported Values:

- **multicast** -- Send advertisements to all-hosts multicast address.
- **broadcast** -- Send advertisements to broadcast address.

advertise-interval

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* advertise-interval *< 1 to 255 >*

  ```
  Usage: vrrp vrid <VRID> advertise-interval <1-255>

  Description: Set time interval (in seconds) between sending VRRP advertisement
               messages. The default value is one second.
  ```

  Range: < 1 to 255 >

all

- [no] vlan *VLAN-ID* ip ospf all

  ```
  Process the request for all IP addresses.
  ```

  Next Available Options:

  - **passive** -- Configures an ospf interface as passive. **(p. 643)**
  - **area** -- Specify an OSPF area.**(p. 622)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 623)**
  - **authentication** -- Disable authentication.**(p. 623)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 638)**
  - **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 626)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 627)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 630)**
  - **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 646)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 649)**
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 652)**

- [no] vlan *VLAN-ID* ip rip all

  ```
  Process the request for all IP addresses.
  ```

  Next Available Options:

  - **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 624)**
  - **authentication-key** -- Set RIP authentication key (maximum 16 characters).**(p. 623)**
  - **metric** < 1 to 15 > -- Set metric for this interface.**(p. 638)**
  - **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 645)**
  - **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 649)**
  - **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 651)**
  - **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 650)**

- vlan *VLAN-ID* connection-rate-filter unblock all

  ```
  Resets all previously blocked by the connection rate filter
  ```

- vlan *VLAN-ID* monitor all *< In | Out | Both >*

  ```
  Monitor all traffic.
  ```

  Supported Values:

  - **In** -- Monitor all inbound traffic
  - **Out** -- Monitor all outbound traffic

- **Both** -- Monitor all inbound and outbound traffic

Next Available Option:

- **mirror** -- Mirror destination.**(p. 639)**

any

- vlan *VLAN-ID* ip pim-dense ip-addr any

  ```
  Dynamically determine IP address.
  ```

- vlan *VLAN-ID* ip pim-sparse ip-addr any

  ```
  Dynamically determine IP address.
  ```

anycast

- [no] vlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* anycast

  ```
  Address that is assigned to a set of interfaces that typically belong to different
  nodes
  ```

area

- vlan *VLAN-ID* ip ospf area

  ```
  Specify an OSPF area.
  ```

  Next Available Options:

  - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 622)**
  - **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 625)**

- vlan *VLAN-ID* ip ospf *IP-ADDR* area

  ```
  Specify an OSPF area.
  ```

  Next Available Options:

  - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 622)**
  - **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 625)**

- vlan *VLAN-ID* ip ospf all area

  ```
  Specify an OSPF area.
  ```

  Next Available Options:

  - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 622)**
  - **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 625)**

area-id

- vlan *VLAN-ID* ip ospf area *OSPF-AREA-ID*

  ```
  Single integer or IP address style dotted decimal.
  ```

- vlan *VLAN-ID* ip ospf *IP-ADDR* area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- vlan *VLAN-ID* ip ospf all area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

authentication

- [no] vlan *VLAN-ID* ip ospf authentication

```
Disable authentication.
```

- [no] vlan *VLAN-ID* ip ospf *IP-ADDR* authentication

```
Disable authentication.
```

- [no] vlan *VLAN-ID* ip ospf all authentication

```
Disable authentication.
```

authentication-key

- vlan *VLAN-ID* ip ospf authentication-key

```
Set simple authentication method and key.
```

Next Available Option:

- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 623)**

- vlan *VLAN-ID* ip ospf authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* authentication-key

```
Set simple authentication method and key.
```

Next Available Option:

- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 623)**

- vlan *VLAN-ID* ip ospf *IP-ADDR* authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

- vlan *VLAN-ID* ip ospf all authentication-key

```
Set simple authentication method and key.
```

Next Available Option:

- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 623)**

- vlan *VLAN-ID* ip ospf all authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

- [no] vlan *VLAN-ID* ip rip authentication-key

```
Set RIP authentication key (maximum 16 characters).
```

Next Available Option:

- **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 624)**

- [no] vlan *VLAN-ID* ip rip *IP-ADDR* authentication-key

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

  Next Available Option:

  - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 624)**

- [no] vlan *VLAN-ID* ip rip all authentication-key

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

  Next Available Option:

  - **auth-key-text** -- Set RIP authentication key (maximum 16 characters). (OCTET-STR) **(p. 624)**

authentication-type

- vlan *VLAN-ID* ip rip authentication-type < *none* | *text* >

  ```
  Set authentication type used on this interface.
  ```

  Supported Values:

  - **none** -- Do not use authentication.
  - **text** -- Use simple password.
- vlan *VLAN-ID* ip rip *IP-ADDR* authentication-type < *none* | *text* >

  ```
  Set authentication type used on this interface.
  ```

  Supported Values:

  - **none** -- Do not use authentication.
  - **text** -- Use simple password.
- vlan *VLAN-ID* ip rip all authentication-type < *none* | *text* >

  ```
  Set authentication type used on this interface.
  ```

  Supported Values:

  - **none** -- Do not use authentication.
  - **text** -- Use simple password.

auth-key-text

- vlan *VLAN-ID* ip rip authentication-key *OCTET-STR*

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

- vlan *VLAN-ID* ip rip *IP-ADDR* authentication-key *OCTET-STR*

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

- vlan *VLAN-ID* ip rip all authentication-key *OCTET-STR*

  ```
  Set RIP authentication key (maximum 16 characters).
  ```

auto

- vlan *VLAN-ID* auto *[ETHERNET] PORT-LIST*

```
Usage: [no] auto [ethernet] PORT-LIST

Description: Cause each port identified in the port list to learn its
             VLAN membership using the GARP VLAN Registration Protocol
             (GVRP). This command is only valid when GVRP is enabled.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- vlan *VLAN-ID* ip igmp auto *[ETHERNET] PORT-LIST*

```
Usage: ip igmp auto [ethernet] PORT-LIST

Description: Instruct the device to monitor incoming multicast traffic
             on the specified ports (this is the default behavior).  This
             feature is configured on a per-VLAN basis.
```

- vlan *VLAN-ID* ipv6 mld auto *[ETHERNET] PORT-LIST*

```
Usage: vlan < vid > ipv6 mld auto < port-list >

Description: Instruct the device to monitor incoming multicast traffic
             on the specified ports (this is the default behavior).  This
             feature is configured on a per-VLAN basis.
```

autoconfig

- [no] vlan *VLAN-ID* ipv6 address autoconfig

```
Automatic address configuration.
```

backbone

- vlan *VLAN-ID* ip ospf area backbone

```
The backbone area (the same as 0.0.0.0).
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* area backbone

```
The backbone area (the same as 0.0.0.0).
```

- vlan *VLAN-ID* ip ospf all area backbone

```
The backbone area (the same as 0.0.0.0).
```

backup

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* backup

```
Usage: vrrp vrid <VRID> backup

Description: Designate the virtual router instance as a Backup.
             There is no default value.
```

blocked

- vlan *VLAN-ID* ip igmp blocked *[ETHERNET] PORT-LIST*

```
Usage: ip igmp blocked [ethernet] PORT-LIST

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

- vlan *VLAN-ID* ipv6 mld blocked *[ETHERNET] PORT-LIST*

```
Usage: vlan < vid > ipv6 mld blocked < port-list >

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

chain-name

- vlan *VLAN-ID* ip ospf md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- vlan *VLAN-ID* ip ospf all md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

connection-rate-filter

- vlan *VLAN-ID* connection-rate-filter

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK
>
       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Re-enables access to a host or set of hosts  that has been previously
             blocked by the connection rate filter. Disabling or setting sensitivity

             may have improved performance after rebooting the switch
```

Next Available Option:

- **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 653)**

cost

- vlan *VLAN-ID* ip ospf cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf all cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

dead-interval

- vlan *VLAN-ID* ip ospf dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >
- vlan *VLAN-ID* ip ospf *IP-ADDR* dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >
- vlan *VLAN-ID* ip ospf all dead-interval *< 1 to 65535 >*

  ```
  Set dead interval in seconds; the default is 40.
  ```

  Range: < 1 to 65535 >

dhcp

- [no] vlan *VLAN-ID* ipv6 address dhcp

  ```
  Configure a DHCPv6 client.
  ```

  Next Available Option:
  - **full** -- Obtain IPv6 address & Configuration information from DHCPv6 server.**(p. 630)**

dhcp-bootp

- vlan *VLAN-ID* ip address dhcp-bootp

  ```
  Configure the interface to use DHCP/Bootp server to acquire parameters.
  ```

dhcp-snooping

- [no] vlan *VLAN-ID* dhcp-snooping

direction

- [no] vlan *VLAN-ID* ip access-group *ACCESS-GROUP* *< in | out | connection-rate-filter | ... >*

  Supported Values:
  - **in** -- Match inbound packets
  - **out** -- Match outbound packets
  - **connection-rate-filter** -- Manage packet rates
  - **vlan** -- VLAN acl

domain-name

- [no] vlan *VLAN-ID* igmp-proxy *< END OF PRINTABLE >*

  ```
  Specify the domain name to associate/disassociate with the VLAN.
  ```

  Supported Values:
  - **END OF PRINTABLE**

dr-priority

- vlan *VLAN-ID* ip pim-sparse dr-priority *INTEGER*

```
Usage: ip pim-sparse dr-priority <0-2147483647>

Description: Set the priority value to use on the interface in the Designated
             Router election process. Default is 1.
```

dscp

- vlan *VLAN-ID* qos dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

Supported Values:

Binary formatted value from 000000 to 111111

enable

- [no] vlan *VLAN-ID* ipv6 enable

```
Enable IPv6 on an interface and configures an automatically generated link-local addr.
```

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* enable

```
Usage: [no] vrrp vrid <VRID> enable

Description: Enable/disable operation of the virtual router instance.
             The default value is 'disabled'.
```

eui-64

- [no] vlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN* eui-64

```
An IPv6 EUI-64 address that can be automatically configured on any interface
```

fastleave

- [no] vlan *VLAN-ID* ip igmp fastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp fastleave [ethernet] PORT-LIST

Description: Enables or disables IGMP Fast Leaves. When enabled, as soon as
             an IGMP Group Leave has been received on a non-cascaded port,
             the switch stops forwarding multicast traffic for that group
             to that port.
             Does not apply to cascaded ports (see ip igmp forcedfastleave).
             When disabled, or when the port is cascaded, the regular IGMP
             leave time is used (up to 10 seconds when the switch is not
             the IGMP Querier).
             The default behavior is for IGMP FastLeaves to be enabled.
             This feature is configured for ports on a per-VLAN basis.
```

- [no] vlan *VLAN-ID* ipv6 mld fastleave *[ETHERNET] PORT-LIST*

```
Usage:  [no] ipv6 mld fastleave < port-list >

Description: Enables MLD fast-leaves on the specified ports in the selected VLAN.
             The no form of the command disables MLD fast-leave on the specified
             ports in the selected VLAN.
```

forbid

- [no] vlan *VLAN-ID* forbid *[ETHERNET] PORT-LIST*

```
Usage: [no] forbid [ethernet] PORT-LIST

Description: Prevent ports from becoming a member of the current VLAN.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

forcedfastleave

- [no] vlan *VLAN-ID* ip igmp forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forcedfastleave [ethernet] PORT-LIST

Description: When enabled, this feature forces IGMP Fast Leaves to occur
             even when the port is cascaded. See 'ip igmp fastleave' for
             more information.  The default behavior is for IGMP Forced
             FastLeaves to be disabled.
             This feature is configured for ports on a per-VLAN basis.
```

- [no] vlan *VLAN-ID* ipv6 mld forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] vlan < vid > ipv6 mld forcedfastleave <port-list>

Description: Enables MLD Forced Fast-Leave on the specified ports in the selected
VLAN,
             even if they are cascaded. (Default: Disabled.)  The no form of the
command
             disables Forced Fast-Leave on the specified ports in the selected VLAN
```

forward

- vlan *VLAN-ID* ip igmp forward *[ETHERNET] PORT-LIST*

```
Usage: ip igmp forward [ethernet] PORT-LIST

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

- vlan *VLAN-ID* ipv6 mld forward *[ETHERNET] PORT-LIST*

```
Usage: vlan < vid > ipv6 mld forward < port-list >

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

forward-protocol

- vlan *VLAN-ID* ip forward-protocol

```
Usage: [no] ip forward-protocol udp IP-ADDR PORT-NUM|PORT-NAME

Description: Add or remove a UDP server address for the VLAN. The
             broadcast  packets received by the switch on this VLAN are to
             be forwarded to the specified application server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **udp** -- Add or remove a UDP server address for the VLAN**(p. 652)**

full

- [no] vlan *VLAN-ID* ipv6 address dhcp full

```
Obtain IPv6 address & Configuration information from DHCPv6 server.
```

Next Available Option:

- **rapid-commit** -- Obtain IPv6 address quickly from DHCPv6 server.**(p. 649)**

graft-retry-interval

- vlan *VLAN-ID* ip pim-dense graft-retry-interval *< 1 to 10 >*

```
Usage: ip pim-dense graft-retry-interval <1-10>

Description: Set the interval a PIM router waits for a Graft Ack before
             resending a Graft on this interface. Default value is 3
             seconds.
```

Range: < 1 to 10 >

hello-delay

- vlan *VLAN-ID* ip pim-dense hello-delay *< 0 to 5 >*

```
Usage: ip pim-dense hello-delay <0-5>

Description: Set the maximum time before a triggered PIM Hello message is
             transmitted on this interface. Default value is 5 seconds.
```

Range: < 0 to 5 >

- vlan *VLAN-ID* ip pim-sparse hello-delay *< 0 to 5 >*

```
Usage: ip pim-sparse hello-delay <0-5>

Description: Set the maximum time before a triggered PIM Hello message is
             transmitted on this interface. Default value is 5 seconds.
```

Range: < 0 to 5 >

hello-interval

- vlan *VLAN-ID* ip ospf hello-interval *< 1 to 65535 >*

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* hello-interval *< 1 to 65535 >*

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf all hello-interval *< 1 to 65535 >*

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip pim-dense hello-interval *< 5 to 300 >*

```
Usage: ip pim-dense hello-interval <5-300>

Description: Set the frequency at which PIM Hello messages are transmitted
             on this interface. Default value is 30 seconds.
```

Range: < 5 to 300 >

- vlan *VLAN-ID* ip pim-sparse hello-interval *< 5 to 300 >*

```
Usage: ip pim-sparse hello-interval <5-300>

Description: Set the frequency at which PIM Hello messages are transmitted
             on this interface. Default value is 30 seconds.
```

Range: < 5 to 300 >

helper-address

- [no] vlan *VLAN-ID* ip helper-address *IP-ADDR*

```
Usage: [no] ip helper-address IP-ADDR

Description: Add or remove a DHCP server IP address for the VLAN. The
             DHCP requests received by the switch on this VLAN are to
             be relayed to the specified DHCP server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

high-priority-forward

- [no] vlan *VLAN-ID* ip igmp high-priority-forward

```
Usage: [no] ip igmp high-priority-forward

Description: Enable/disable the high priority forwarding of traffic for
             subscribed IP Multicast groups. This feature is configured on
             a per-VLAN  basis.
```

holdtime

- vlan *VLAN-ID* ip irdp holdtime *< 4 to 9000 >*

```
Usage: [no] ip irdp holdtime <4-9000>

Description: Set the lifetime (in seconds) of the router advertisements sent
             on this interface. Must be no less than the maximum time
             allowed between sending unsolicited router advertisements.
```

Range: < 4 to 9000 >

host

- vlan *VLAN-ID* connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

igmp

- [no] vlan *VLAN-ID* ip igmp

```
Usage: [no] ip igmp [...]

Description: Enable/disable/configure IP Multicast Group Protocol (IGMP)
             feature on a VLAN.  This command enables, disables or
             configures the IGMP feature for IGMP communication between
             Multicast Routers, Multicast Servers, and Multicast Clients
             connected to the device.  This is a VLAN context command. It
             can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix.  If not preceded by 'no',
             the command accepts a variety of configuration parameters. To
             get a list of all available parameters use 'ip igmp ?'. To
             get detailed help for a parameter follow it with 'help'
             keyword.
```

Next Available Options:

- **querier** -- Specify querier/non-querier capability for the VLAN**(p. 648)**
- **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups**(p. 631)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 625)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 625)**
- **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 628)**
- **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 629)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 629)**

igmp-proxy

- [no] vlan *VLAN-ID* igmp-proxy

```
Usage: [no] igmp-proxy DOMAIN-NAME

Description: Associate an IGMP proxy domain with a VLAN.
             If the 'no' keyword is used:
                 If the DOMAIN-NAME is left blank, all the domains
                 associated with the respective VLAN will be disassociated.
                 If a DOMAIN-NAME is specified, The specified domain will
                 be disassociated from the respecive VLAN.
             If the 'no' keyword is not used:
                 If the DOMAIN-NAME matches the domain name of an
                 existing domain, the respective domain will be associated
                 with the respective VLAN.
```

Next Available Option:

- **domain-name** < END OF PRINTABLE > -- Specify the domain name to associate/disassociate with the VLAN. (ASCII-STR) **(p. 627)**

interval

- vlan *VLAN-ID* ip igmp querier interval *< 5 to 300 >*

```
Sets the interval in seconds between IGMP queries
 (default: 125)
```

Range: < 5 to 300 >

- vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR* interval

```
Specify the L3-Mac-Address timeout interval.
```

Next Available Option:

- **timer-interval** < 1 to 255 > -- Timeout interval in seconds <1-255>. **(p. 652)**

ip

- vlan *VLAN-ID* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the VLAN. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 618)**
- **address** -- Set IP parameters for communication within an IP network**(p. 619)**
- **proxy-arp** -- Enable/disable proxy ARP**(p. 648)**
- **local-proxy-arp** -- Enable/disable local proxy ARP**(p. 637)**
- **helper-address** -- Add or remove a DHCP server IP address for the VLAN (IP-ADDR) **(p. 631)**
- **forward-protocol** -- Add or remove a UDP server address for the VLAN**(p. 629)**
- **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature on a VLAN**(p. 632)**
- **irdp** -- Configure ICMP Router Discovery Protocol (IRDP)**(p. 636)**
- **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the VLAN interface**(p. 642)**
- **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the VLAN interface**(p. 650)**
- **pim-dense** -- Enable/disable/configure PIM-DM protocol on the VLAN interface**(p. 643)**
- **pim-sparse** -- Enable/disable/configure PIM-SM protocol on the VLAN interface**(p. 644)**
- **mroute** -- Configure IP Multicast Routing parameters on the VLAN interface**(p. 641)**

- [no] vlan *VLAN-ID* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:

- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 618)**

ip-addr

- [no] vlan *VLAN-ID* ip address *IP-ADDR/MASK-LENGTH*

```
Interface IP address/mask.
```

- [no] vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR*

  ```
  IP address of the protocol server.
  ```

  Next Available Options:
  - **port-num** -- UDP port number of the server. (TCP/UDP-PORT) **(p. 645)**
  - **port-name** < dns | ntp | netbios-ns | ... > -- (NUMBER) **(p. 645)**

- [no] vlan *VLAN-ID* ip ospf *IP-ADDR*

  ```
  Specify the IP address the request is for.
  ```

  Next Available Options:
  - **passive** -- Configures an ospf interface as passive. **(p. 643)**
  - **area** -- Specify an OSPF area.**(p. 622)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 623)**
  - **authentication** -- Disable authentication.**(p. 623)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 638)**
  - **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 626)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 627)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 630)**
  - **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 646)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 649)**
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 652)**

- [no] vlan *VLAN-ID* ip rip *IP-ADDR*

  ```
  Specify the IP address the request is for.
  ```

  Next Available Options:
  - **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 624)**
  - **authentication-key** -- Set RIP authentication key (maximum 16 characters).**(p. 623)**
  - **metric** < 1 to 15 > -- Set metric for this interface.**(p. 638)**
  - **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 645)**
  - **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 649)**
  - **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 651)**
  - **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 650)**

- vlan *VLAN-ID* ip pim-dense ip-addr

  ```
  Usage: ip pim-dense [ip-addr IP-ADDR|any]

  Description: Set the source IP address for the PIM-DM packets sent out on this
               interface. You can either explicitly specify one of the existing
               VLAN's IP addresses or use 'any' option to dynamically determine
               it from the VLAN's current IP configuration. The default is 'any'.
               This command also enable the PIM-DM protocol on the VLAN interface.
  ```

  Next Available Options:
  - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 633)**
  - **any** -- Dynamically determine IP address.**(p. 622)**

- vlan *VLAN-ID* ip pim-dense ip-addr *IP-ADDR*

```
Specify IP address.
```

- vlan *VLAN-ID* ip pim-sparse ip-addr

```
Usage: ip pim-sparse [ip-addr IP-ADDR|any]

Description: Set the source IP address for the PIM-SM packets sent out on this
             interface. You can either explicitly specify one of the existing
             VLAN's IP addresses or use 'any' option to dynamically determine
             it from the VLAN's current IP configuration. The default is 'any'.
             This command also enable the PIM-SM protocol on the VLAN interface.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 633)**
- **any** -- Dynamically determine IP address.**(p. 622)**

- vlan *VLAN-ID* ip pim-sparse ip-addr *IP-ADDR*

```
Specify IP address.
```

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* virtual-ip-address *IP-ADDR/MASK-LENGTH*

```
Specify IP address/mask.
```

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address *IP-ADDR*

```
Specify IP address.
```

ip-recv-mac-address

- [no] vlan *VLAN-ID* ip-recv-mac-address

```
Usage: [no] ip-recv-mac-address <macaddress> interval <1-255>

Description:  Associates a L3-mac-address with a VLAN.
      To associate L3-Mac-Address for a VLAN.
         ip-recv-mac-address <mac-address> interval <1-255>
      To associate L3-Mac-Address with a VLAN with default
      timeout interval of 60s.
         ip-recv-mac-address <mac-address>
      To disassociate L3-Mac_address with a VLAN.
             no ip-recv-mac-address
Parameters:
       <mac-address>  -  The L3-mac-address to be associated with a VLAN.
       interval       -  Specify L3-Mac-Address timeout interval.
       <1-255>        -  Timeout interval in seconds <1-255>.
```

Next Available Option:

- **mac-address** -- The L3-mac-address to be associated with a VLAN. (MAC-ADDR) **(p. 638)**

ipv6

- vlan *VLAN-ID* ipv6

```
Usage: [no] ipv6 ...

Description: Configure various IP parameters for the VLAN. The 'ipv6'
             command must be followed by a feature-specific keyword.
             Use 'ipv6 ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **enable** -- Enable IPv6 on an interface and configures an automatically generated link-local addr.**(p. 628)**
- **address** -- Set IPv6 parameters for communication within an IP network**(p. 619)**
- **mld** -- Enable/disable/configure IPv6 Multicast Listener Discovery (MLD) feature on a VLAN**(p. 639)**

ipv6-addr

- [no] vlan *VLAN-ID* ipv6 address *IPV6-ADDR*

```
Configure a link-local IPv6 address.
```

Next Available Option:

- **link-local** -- Configure a link-local IPv6 address.**(p. 637)**

ipv6-addr/mask

- [no] vlan *VLAN-ID* ipv6 address *IPV6-ADDR/PREFIX-LEN*

```
Configure IPv6 address represented in CIDR notation.
```

Next Available Options:

- **anycast** -- Address that is assigned to a set of interfaces that typically belong to different nodes**(p. 622)**
- **eui-64** -- An IPv6 EUI-64 address that can be automatically configured on any interface**(p. 628)**

irdp

- [no] vlan *VLAN-ID* ip irdp

```
Usage: [no] ip irdp [...]

Description: Configure ICMP Router Discovery Protocol (IRDP). This is
             a VLAN context command. It can be called directly from the VLAN
             context or may follow the 'vlan VLAN-ID' command prefix.
             Called without parameters the command enables or disables (if
             preceded by 'no') the protocol on the VLAN specified, or
             identified by the current VLAN context. Use 'ip irdp ?' to get
             a list of all possible configurable parameters.
```

Next Available Options:

- **advert-address** < multicast | broadcast > -- Specify the destination address to be used for router advertisements**(p. 620)**
- **holdtime** < 4 to 9000 > -- Set the lifetime (in seconds) of the router advertisements sent on this interface**(p. 631)**

- **maxadvertinterval** < 4 to 1800 > -- Set the maximum time (in seconds) allowed between sending unsolicited router advertisements**(p. 638)**
- **minadvertinterval** < 3 to 1800 > -- Set the minimum time (in seconds) allowed between sending unsolicited router advertisements**(p. 639)**
- **preference** -- The preferability of the router as a default router, relative to the other routers on the same subnet**(p. 646)**

jumbo

- [no] vlan *VLAN-ID* jumbo

```
Usage: [no] jumbo

Description: Labels this VLAN as a Jumbo VLAN, allowing you to pass
             packets up to 9220 bytes in size.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

lan-prune-delay

- [no] vlan *VLAN-ID* ip pim-dense lan-prune-delay

```
Usage: [no] ip pim-dense lan-prune-delay

Description: Turn on/off the LAN Prune Delay Option on this interface.
             Default is 'on'.
```

- [no] vlan *VLAN-ID* ip pim-sparse lan-prune-delay

```
Usage: [no] ip pim-sparse lan-prune-delay

Description: Turn on/off the LAN Prune Delay Option on this interface.
             Default is 'on'.
```

link-local

- [no] vlan *VLAN-ID* ipv6 address *IPV6-ADDR* link-local

```
Configure a link-local IPv6 address.
```

local-proxy-arp

- [no] vlan *VLAN-ID* ip local-proxy-arp

```
Usage: [no] ip local-proxy-arp

Description: Enable/disable local proxy ARP. This is a VLAN context command.
             It can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix. When local proxy ARP is
             enabled on a VLAN, the device responds to all ARP requests
             received on the VLAN ports with it's own hardware address.
```

lowest

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address lowest

```
Dynamically determine lowest IP address.
```

mac-address

- vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR*

  ```
  The L3-mac-address to be associated with a VLAN.
  ```

  Next Available Option:
  - **interval** -- Specify the L3-Mac-Address timeout interval. **(p. 632)**

maxadvertinterval

- vlan *VLAN-ID* ip irdp maxadvertinterval *< 4 to 1800 >*

  ```
  Usage: [no] ip irdp maxadvertinterval <4-1800>

  Description: Set the maximum time (in seconds) allowed between sending
               unsolicited router advertisements.
  ```

  Range: < 4 to 1800 >

max-graft-retries

- vlan *VLAN-ID* ip pim-dense max-graft-retries *< 1 to 10 >*

  ```
  Usage: ip pim-dense max-graft-retries <1-10>

  Description: Set the maximum number of times this router will resend a
               Graft on this interface. Default is 2.
  ```

  Range: < 1 to 10 >

md5-auth-key-chain

- vlan *VLAN-ID* ip ospf md5-auth-key-chain

  ```
  Set MD5 authentication method and key chain.
  ```

  Next Available Option:
  - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 626)**

- vlan *VLAN-ID* ip ospf *IP-ADDR* md5-auth-key-chain

  ```
  Set MD5 authentication method and key chain.
  ```

  Next Available Option:
  - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 626)**

- vlan *VLAN-ID* ip ospf all md5-auth-key-chain

  ```
  Set MD5 authentication method and key chain.
  ```

  Next Available Option:
  - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 626)**

metric

- vlan *VLAN-ID* ip rip metric *< 1 to 15 >*

```
Set metric for this interface.
```

Range: < 1 to 15 >

- vlan *VLAN-ID* ip rip *IP-ADDR* metric *< 1 to 15 >*

  ```
  Set metric for this interface.
  ```

  Range: < 1 to 15 >

- vlan *VLAN-ID* ip rip all metric *< 1 to 15 >*

  ```
  Set metric for this interface.
  ```

  Range: < 1 to 15 >

minadvertinterval

- vlan *VLAN-ID* ip irdp minadvertinterval *< 3 to 1800 >*

  ```
  Usage: [no] ip irdp minadvertinterval <3-1800>

  Description: Set the minimum time (in seconds) allowed between sending
               unsolicited router advertisements. Must be no greater than the
               maximum time between sending unsolicited router advertisements.
  ```

  Range: < 3 to 1800 >

mirror

- vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror

  ```
  Mirror destination.
  ```

  Next Available Options:

  - **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 641)**
  - **mirror_session_name** -- Mirror destination name.**(p. 639)**

- vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror

  ```
  Mirror destination.
  ```

  Next Available Options:

  - **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 641)**
  - **mirror_session_name** -- Mirror destination name.**(p. 639)**

mirror_session_name

- [no] vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror

  ```
  Mirror destination name.
  ```

- [no] vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror

  ```
  Mirror destination name.
  ```

mld

- [no] vlan *VLAN-ID* ipv6 mld

```
Usage: [no] ipv6 mld [...]

Description: Enable/disable/configure IPv6 Multicast Listener Discovery (MLD)
             feature on a VLAN.  This command enables, disables or
             configures the MLD feature for MLD communication between
             Multicast Routers, Multicast Servers, and Multicast Clients
             connected to the device.  This is a VLAN context command.
             If not preceded by 'no',
             the command accepts a variety of configuration parameters. To
             get a list of all available parameters use 'ipv6 mld ?'. To
             get detailed help for a parameter follow it with 'help'
             keyword.

Example Commands:
             ProCurve(vlan-8)# ipv6 mld forward a16-a18
             ProCurve(vlan-8)# ipv6 mld blocked a19-a21
             ProCurve(vlan-8)# show ipv6 mld vlan 8 config
```

Next Available Options:

- **querier** -- This command disables or re-enables the ability for the switch to become querier if necessary**(p. 648)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 625)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 625)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 629)**
- **fastleave** -- Enables MLD fast-leaves on the specified ports in the selected VLAN ([ethernet] PORT-LIST) **(p. 628)**
- **forcedfastleave** -- Enables MLD Forced Fast-Leave on the specified ports in the selected VLAN, even if they are cascaded ([ethernet] PORT-LIST) **(p. 629)**

monitor

- [no] vlan *VLAN-ID* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
              [1-4 | NAME-STR]...
       2) [no] monitor ip access-group <ACL-NAME> <in> mirror
              <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the VLAN is to be monitored or not.
             The network traffic seen by the monitored VLAN is copied to
             the Mirroring Destination to which a network analyzer can be
             attached.
             Note: When mirroring a VLAN in a busy network,
             some frames may not be copied to the mirroring port.
             This is an VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID command.

Parameters:  o 1-4 - Mirror destination number
             o NAME-STR - Friendly name associated with the mirror
             destination number.
             o ACL-NAME - Standard or Extended Access Control List number.
             o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 621)**
- **ip** -- Apply an IPv4 access list.**(p. 633)**

monitor_mirror_ACL_dir

- vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 639)**

monitor_mirror_session_id

- [no] vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

mroute

- vlan *VLAN-ID* ip mroute

```
Usage: ip mroute ...

Description: Configure IP Multicast Routing parameters on the VLAN
             interface. The command must be followed by a parameter.
             Use 'ip mroute ?' to get a list of all possible parameters.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **ttl-threshold** < 0 to 255 > -- Set the multicast datagram TTL threshold for the interface**(p. 652)**

name

- vlan *VLAN-ID* name *NAME*

```
Usage: name ASCII-STR

Description: Set the VLAN's name.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

nbr-timeout

- vlan *VLAN-ID* ip pim-sparse nbr-timeout *< 60 to 8000 >*

```
Usage: ip pim-sparse nbr-timeout <60-8000>

Description: Set the neighbour loss time interval for this interface.
             Default is 180 seconds.
```

Range: < 60 to 8000 >

no-default

- vlan *VLAN-ID* ip irdp preference no-default

```
Indicates that the router should never be used as a default by its neighbors.
```

number

- vlan *VLAN-ID* ip irdp preference *< -2147483647 to 2147483647 >*

```
The router preferability number. Higher values are more preferable.
```

Range: < -2147483647 to 2147483647 >

ospf

- [no] vlan *VLAN-ID* ip ospf

```
Usage: [no] ip ospf [...]

Description: Enable/disable/configure Open Shortest Path First (OSPF)
             protocol on the VLAN interface.
             Called without 'no', the command enables OSPF on the interface.
             Otherwise ('no' is specified), the command disables OSPF on the
             interface. The command can be followed by an OSPF configuration
             command. Use 'ip ospf ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **passive** -- Configures an ospf interface as passive. **(p. 643)**
- **area** -- Specify an OSPF area.**(p. 622)**
- **authentication-key** -- Set simple authentication method and key.**(p. 623)**
- **authentication** -- Disable authentication.**(p. 623)**

- **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 638)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 626)**
- **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 627)**
- **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 630)**
- **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 646)**
- **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 649)**
- **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 652)**
- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 633)**
- **all** -- Process the request for all IP addresses.**(p. 621)**

override-interval

- vlan *VLAN-ID* ip pim-dense override-interval *< 500 to 6000 >*

```
Usage: ip pim-dense override-interval <500-6000>

Description: Set the value inserted into the Override Interval field of
             a LAN Prune Delay option on this interface. Default is 2500
             milliseconds.
```

  Range: < 500 to 6000 >

- vlan *VLAN-ID* ip pim-sparse override-interval *< 500 to 6000 >*

```
Usage: ip pim-sparse override-interval <500-6000>

Description: Set the value inserted into the Override Interval field of
             a LAN Prune Delay option on this interface. Default is 2500
             milliseconds.
```

  Range: < 500 to 6000 >

owner

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* owner

```
Usage: vrrp vrid <VRID> owner

Description: Designate the virtual router instance as an Owner (Master).
             There is no default value.
```

passive

- [no] vlan *VLAN-ID* ip ospf passive

```
Configures an ospf interface as passive.
```

- [no] vlan *VLAN-ID* ip ospf *IP-ADDR* passive

```
Configures an ospf interface as passive.
```

- [no] vlan *VLAN-ID* ip ospf all passive

```
Configures an ospf interface as passive.
```

pim-dense

- [no] vlan *VLAN-ID* ip pim-dense

```
Usage: [no] ip pim-dense [...]

Description: Enable/disable/configure PIM-DM protocol on the VLAN interface.
             Use direct and 'no' versions of the command to enable/disable
             PIM-DM on the interface. Use 'ip pim-dense ?' to get the list
             of all configuration options. This command can be used in the
             VLAN context or in the global context with the 'vlan <VLAN-ID>'
             prefix.
```

Next Available Options:

- **ip-addr** -- Set the source IP address for the PIM-DM packets sent out on this interface**(p. 633)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface**(p. 637)**
- **hello-interval** < 5 to 300 > -- Set the frequency at which PIM Hello messages are transmitted on this interface**(p. 630)**
- **hello-delay** < 0 to 5 > -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface**(p. 630)**
- **graft-retry-interval** < 1 to 10 > -- Set the interval a PIM router waits for a Graft Ack before resending a Graft on this interface**(p. 630)**
- **max-graft-retries** < 1 to 10 > -- Set the maximum number of times this router will resend a Graft on this interface**(p. 638)**
- **override-interval** < 500 to 6000 > -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface**(p. 643)**
- **propagation-delay** < 250 to 2000 > -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface**(p. 647)**
- **ttl-threshold** < 0 to 255 > -- Set the Time To Live in a PIM-DM State Refresh message at which it is not forwarded on this interface**(p. 652)**

pim-sparse

- [no] vlan *VLAN-ID* ip pim-sparse

```
Usage: [no] ip pim-sparse [...]

Description: Enable/disable/configure PIM-SM protocol on the VLAN interface.
             Use direct and 'no' versions of the command to enable/disable
             PIM-SM on the interface. Use 'ip pim-sparse ?' to get the list
             of all configuration options. This command can be used in the
             VLAN context or in the global context with the 'vlan <VLAN-ID>'
             prefix.
```

Next Available Options:

- **ip-addr** -- Set the source IP address for the PIM-SM packets sent out on this interface**(p. 633)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface**(p. 637)**
- **hello-interval** < 5 to 300 > -- Set the frequency at which PIM Hello messages are transmitted on this interface**(p. 630)**
- **hello-delay** < 0 to 5 > -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface**(p. 630)**
- **override-interval** < 500 to 6000 > -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface**(p. 643)**
- **propagation-delay** < 250 to 2000 > -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface**(p. 647)**
- **dr-priority** -- Set the priority value to use on the interface in the Designated Router election process**(p. 627)**
- **nbr-timeout** < 60 to 8000 > -- Set the neighbour loss time interval for this interface**(p. 642)**

poison-reverse

- [no] vlan *VLAN-ID* ip rip poison-reverse

```
Enable/disable poison reverse on this interface.
```

- [no] vlan *VLAN-ID* ip rip *IP-ADDR* poison-reverse

```
Enable/disable poison reverse on this interface.
```

- [no] vlan *VLAN-ID* ip rip all poison-reverse

```
Enable/disable poison reverse on this interface.
```

port-name

- [no] vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR < dns | ntp | netbios-ns | ... >*

  Supported Values:
  - **dns** -- Domain Name Service (53)
  - **ntp** -- Network Time Protocol (123)
  - **netbios-ns** -- NetBIOS Name Service (137)
  - **netbios-dgm** -- NetBIOS Datagram Service (138)
  - **radius** -- Remote Authentication Dial-In User Service (1812)
  - **radius-old** -- Remote Authentication Dial-In User Service (1645)
  - **rip** -- Routing Information Protocol (520)
  - **snmp** -- Simple Network Management Protocol (161)
  - **snmp-trap** -- Simple Network Management Protocol (162)
  - **tftp** -- Trivial File Transfer Protocol (69)
  - **timep** -- Time Protocol (37)

port-num

- [no] vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR TCP/UDP-PORT*

```
UDP port number of the server.
```

preempt-delay-time

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* preempt-delay-time *< 1 to 600 >*

```
Usage: [no] vrrp vrid <VRID> preempt-delay-time <1-600>

Description: Allows you to specify a time in seconds that the Owner router
             will wait before taking control of the virtual IP address and
             beginning to route packets. You can configure the time on VRRP
             Owner and Backup routers.
             The "no" form of the command may be used to disable the
             pre-emptive delay timer.

Note:        If you have configured the Preempt Delay Timer with a non-zero
             value, you must use the "no" form of the command to change it
             to zero.

Parameters:

    o preempt-delay-time <1-600> - The number of seconds to delay.
```

Range: < 1 to 600 >

preempt-mode

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* preempt-mode

```
Usage: [no] vrrp vrid <VRID> preempt-mode

Description: Enable/disable preempt mode for the virtual router instance.
             The default value is 'enabled'.
```

preference

- vlan *VLAN-ID* ip irdp preference

```
Usage: [no] ip irdp preference <no-default|<-2147483647-2147483647>>

Description: The preferability of the router as a default
             router, relative to the other routers on the same
             subnet.  Higher values are more preferable.
```

Next Available Options:

- **number** < -2147483647 to 2147483647 > -- The router preferability number. Higher values are more preferable.**(p. 642)**
- **no-default** -- Indicates that the router should never be used as a default by its neighbors.**(p. 642)**

primary-ip-address

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address

```
Usage: [no] vrrp vrid <VRID> primary-ip-address <IP-ADDR | lowest>

Description: Specify IP address the virtual router instance will use as
             a source in VRRP advertisement messages. If not set (i.e. is
             '0.0.0.0') the virtual router uses numerically lowest IP address
             of the VLAN. The default value is 'lowest'.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 633)**
- **lowest** -- Dynamically determine lowest IP address.**(p. 637)**

priority

- vlan *VLAN-ID* ip ospf priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* ip ospf all priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* qos priority *< 0 | 1 | 2 | ... >*

  ```
  Specify priority to use.
  ```

  Supported Values:

  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* priority *< 1 to 255 >*

  ```
  Usage: vrrp vrid <VRID> priority <1-255>

  Description: Configure priority for the virtual router instance.
               The default value is '100'.
  ```

  Range: < 1 to 255 >

propagation-delay

- vlan *VLAN-ID* ip pim-dense propagation-delay *< 250 to 2000 >*

  ```
  Usage: ip pim-dense propagation-delay <250-2000>

  Description: Set the value inserted into the LAN Prune Delay field of a
               LAN Prune Delay option on this interface. Default is 500
               milliseconds.
  ```

  Range: < 250 to 2000 >
- vlan *VLAN-ID* ip pim-sparse propagation-delay *< 250 to 2000 >*

  ```
  Usage: ip pim-sparse propagation-delay <250-2000>

  Description: Set the value inserted into the LAN Prune Delay field of a
               LAN Prune Delay option on this interface. Default is 500
               milliseconds.
  ```

  Range: < 250 to 2000 >

protocol

- vlan *VLAN-ID* protocol

  ```
  Set a predefined protocol for the current VLAN.
  ```

  Next Available Options:

  - **protocols** < IPX | IPv4 | IPv6 | ... > -- Set a predefined protocol for the current VLAN. **(p. 648)**
  - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 647)**

protocol-group

- [no] vlan *VLAN-ID* protocol *PROTOCOL-GROUP*

```
Enter a list of protocols for the current VLAN delimited by commas.
```

protocols

- [no] vlan *VLAN-ID* protocol *< IPX | IPv4 | IPv6 | ... >*

```
Set a predefined protocol for the current VLAN.
```

Supported Values:

- **IPX** -- IPX Protocol Group
- **IPv4** -- IP version 4 Protocol Group
- **IPv6** -- IP version 6 Protocol Group
- **ARP** -- Address Resolution Protocol Group
- **Appletalk** -- Appletalk Protocol Group
- **SNA** -- System Network Architecture Protocol Group
- **NetBEUI** -- Network BIOS Enhanced User Interface Protocol Group

proxy-arp

- [no] vlan *VLAN-ID* ip proxy-arp

```
Usage: [no] ip proxy-arp

Description: Enable/disable proxy ARP. This is a VLAN context command.
             It can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix. When proxy ARP is enabled on
             a VLAN, the device responds to ARP requests received on the
             VLAN ports when the device knows a route to the requested IP
             addresses.
```

qos

- [no] vlan *VLAN-ID* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]

Description: Set VLAN-based priority. The 'dscp' or 'priority' must
             be specified if 'no' is not used. Using 'no' configures
             the switch not to apply a VLAN priority override to this
             VLAN's packets.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 628)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 646)**

querier

- [no] vlan *VLAN-ID* ip igmp querier

```
Usage: [no] ip igmp querier [interval <seconds>]

Description: Specify querier/non-querier capability for the VLAN. IGMP
             queries are not sent when the mode is disabled. When
             enabled, the device cannot become Querier for the subnet
             unless the VLAN has an IP Address (use the 'show ip' command
             to determine this).  Each subnet must have at least one IGMP
             Querier-capable device in order for IGMP to function
             properly.  The querier interval setting modifies the time (in
             seconds) between IGMP queries.
```

Next Available Option:

- **interval** < 5 to 300 > -- Sets the interval in seconds between IGMP queries (default: 125) **(p. 632)**

- [no] vlan *VLAN-ID* ipv6 mld querier

```
Usage: [no] vlan < vid > ipv6 mld querier

Description: This command disables or re-enables the ability for the switch
             to become querier if necessary. The no version of the command
             disables the querier function on the switch.
             The show ipv6 mld config command displays the current querier
             command. (Default Querier Capability: Enabled.)
```

rapid-commit

- [no] vlan *VLAN-ID* ipv6 address dhcp full rapid-commit

```
Obtain IPv6 address quickly from DHCPv6 server.
```

receive

- vlan *VLAN-ID* ip rip receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:

- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

- vlan *VLAN-ID* ip rip *IP-ADDR* receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:

- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

- vlan *VLAN-ID* ip rip all receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:

- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

retransmit-interval

- vlan *VLAN-ID* ip ospf retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- vlan *VLAN-ID* ip ospf all retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

rip

- [no] vlan *VLAN-ID* ip rip

```
Usage: [no] ip rip [...]

Description: Enable/disable/configure Routing Internet Protocol (RIP)
             on the VLAN interface.
             Called without 'no', the command enables RIP on the interface.
             Otherwise ('no' is specified), the command disables RIP on the
             interface. The command can be followed by a RIP configuration
             command. Use 'ip rip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 624)**
- **authentication-key** -- Set RIP authentication key (maximum 16 characters).**(p. 623)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 638)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 645)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 649)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 651)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 650)**
- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 633)**
- **all** -- Process the request for all IP addresses.**(p. 621)**

rip-compatible

- vlan *VLAN-ID* ip rip *< V1-only | V2-only | V1-or-V2 >*

```
Define RIP version for incoming and outgoing packets.
```

Supported Values:

- **V1-only** -- Use RIP version 1 only.
- **V2-only** -- Use RIP version 2 only.
- **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

- vlan *VLAN-ID* ip rip *IP-ADDR* *< V1-only | V2-only | V1-or-V2 >*

```
Define RIP version for incoming and outgoing packets.
```

Supported Values:
- **V1-only** -- Use RIP version 1 only.
- **V2-only** -- Use RIP version 2 only.
- **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

- vlan *VLAN-ID* ip rip all *< V1-only | V2-only | V1-or-V2 >*

```
Define RIP version for incoming and outgoing packets.
```

Supported Values:
- **V1-only** -- Use RIP version 1 only.
- **V2-only** -- Use RIP version 2 only.
- **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

send

- vlan *VLAN-ID* ip rip send *< disabled | V1-only | V1-compatible-V2 | ... >*

```
Define RIP version for outgoing packets.
```

Supported Values:
- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

- vlan *VLAN-ID* ip rip *IP-ADDR* send *< disabled | V1-only | V1-compatible-V2 | ... >*

```
Define RIP version for outgoing packets.
```

Supported Values:
- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

- vlan *VLAN-ID* ip rip all send *< disabled | V1-only | V1-compatible-V2 | ... >*

```
Define RIP version for outgoing packets.
```

Supported Values:
- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

src-ip

- vlan *VLAN-ID* connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

tagged

- [no] vlan *VLAN-ID* tagged *[ETHERNET] PORT-LIST*

```
Usage: [no] tagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as tagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

timer-interval

- vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR* interval *< 1 to 255 >*

  ```
  Timeout interval in seconds <1-255>.
  ```

  Range: < 1 to 255 >

transit-delay

- vlan *VLAN-ID* ip ospf transit-delay *< 1 to 3600 >*

  ```
  Set transit delay in seconds; the default is 1.
  ```

  Range: < 1 to 3600 >
- vlan *VLAN-ID* ip ospf *IP-ADDR* transit-delay *< 1 to 3600 >*

  ```
  Set transit delay in seconds; the default is 1.
  ```

  Range: < 1 to 3600 >
- vlan *VLAN-ID* ip ospf all transit-delay *< 1 to 3600 >*

  ```
  Set transit delay in seconds; the default is 1.
  ```

  Range: < 1 to 3600 >

ttl-threshold

- vlan *VLAN-ID* ip pim-dense ttl-threshold *< 0 to 255 >*

  ```
  Usage: ip pim-dense ttl-threshold <0-255>

  Description: Set the Time To Live in a PIM-DM State Refresh message at
               which it is not forwarded on this interface. Default is 0.
  ```

  Range: < 0 to 255 >
- vlan *VLAN-ID* ip mroute ttl-threshold *< 0 to 255 >*

  ```
  Usage: ip mroute ttl-threshold <0-255>

  Description: Set the multicast datagram TTL threshold for the interface.
               Any IP multicast datagrams with a TTL less than this threshold
               will not be forwarded out the interface. The default value of 0
               means all multicast packets are forwarded out the interface.
  ```

  Range: < 0 to 255 >

udp

- [no] vlan *VLAN-ID* ip forward-protocol udp

  ```
  Usage: [no] ip forward-protocol udp IP-ADDR PORT-NUM|PORT-NAME

  Description: Add or remove a UDP server address for the VLAN. The
               broadcast  packets received by the switch on this VLAN are to
               be forwarded to the specified application server.
               This is a VLAN context command. It can be called directly
               from the VLAN context or follow the 'vlan VLAN-ID'
               command.
  ```

  Next Available Option:

  - **ip-addr** -- IP address of the protocol server. (IP-ADDR) **(p. 633)**

unblock

- vlan *VLAN-ID* connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 621)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 631)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 651)**

untagged

- [no] vlan *VLAN-ID* untagged *[ETHERNET] PORT-LIST*

```
Usage: [no] untagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as untagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

virtual-ip-address

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* virtual-ip-address

```
Usage: [no] vrrp vrid <VRID> virtual-ip-address <IP-ADDR>

Description: Specify IP address to be supported by the virtual router instance.
             There is no default value.
```

Next Available Option:

- **ip-addr** -- Specify IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 633)**

voice

- [no] vlan *VLAN-ID* voice

```
Usage: [no] voice

Description: Labels this VLAN as a Voice VLAN, allowing you to separate,
             prioritize, and authenticate voice traffic moving through
             your network.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

vrid

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >*

```
Usage: [no] vrrp vrid <VRID> [...]

Description: Configure a virtual router instance for the VLAN.
             A virtual router is defined by its virtual router
             identifier (VRID) and a set of IP addresses for which
```

```
                virtual router acts as a Master or Backup. The scope
                of each virtual router is restricted to a single VLAN.
```

Range: < 1 to 255 >

Next Available Options:

- **backup** -- Designate the virtual router instance as a Backup**(p. 625)**
- **owner** -- Designate the virtual router instance as an Owner (Master)**(p. 643)**
- **virtual-ip-address** -- Specify IP address to be supported by the virtual router instance**(p. 653)**
- **primary-ip-address** -- Specify IP address the virtual router instance will use as a source in VRRP advertisement messages**(p. 646)**
- **advertise-interval** < 1 to 255 > -- Set time interval (in seconds) between sending VRRP advertisement messages**(p. 621)**
- **priority** < 1 to 255 > -- Configure priority for the virtual router instance**(p. 646)**
- **preempt-mode** -- Enable/disable preempt mode for the virtual router instance**(p. 646)**
- **preempt-delay-time** < 1 to 600 > -- Enable the pre-emptive delay timer for the virtual router instance**(p. 645)**
- **enable** -- Enable/disable operation of the virtual router instance**(p. 628)**

vrrp

- [no] vlan *VLAN-ID* vrrp

```
Usage: [no] vlan <VLAN-ID> vrrp vrid <VRID> [...]

Description: Enable/disable/configure VRRP operation on the VLAN.
             Use 'vrrp vrid <VRID> ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly from
             the VLAN context or follow the 'vlan VLAN-ID' command.
```

Next Available Option:

- **vrid** < 1 to 255 > -- Configure a virtual router instance for the VLAN**(p. 653)**

walkMIB

OVERVIEW

Category:	SNMP
Primary context:	manager
Related Commands	**getMIB (page 179)** **setMIB (page 430)**

```
Usage: walkmib OBJECT-STR [OBJECT-STR ...]

Description: Walk through all instances of the object specified displaying
             the MIB object names, instances and values.
```

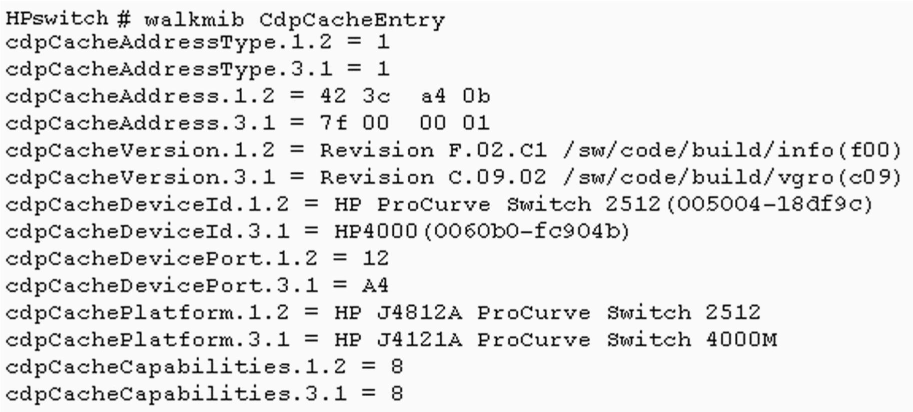
COMMAND STRUCTURE

- walkMIB **object** -- The mib object to start from. (ASCII-STR) **(p. 655)**

EXAMPLES

Example: walkMIB

Walk the MIB objects in CdpCacheEntry:



```
HPswitch # walkmib CdpCacheEntry
cdpCacheAddressType.1.2 = 1
cdpCacheAddressType.3.1 = 1
cdpCacheAddress.1.2 = 42 3c  a4 0b
cdpCacheAddress.3.1 = 7f 00  00 01
cdpCacheVersion.1.2 = Revision F.02.C1 /sw/code/build/info(f00)
cdpCacheVersion.3.1 = Revision C.09.02 /sw/code/build/vgro(c09)
cdpCacheDeviceId.1.2 = HP ProCurve Switch 2512(005004-18df9c)
cdpCacheDeviceId.3.1 = HP4000(0060b0-fc904b)
cdpCacheDevicePort.1.2 = 12
cdpCacheDevicePort.3.1 = A4
cdpCachePlatform.1.2 = HP J4812A ProCurve Switch 2512
cdpCachePlatform.3.1 = HP J4121A ProCurve Switch 4000M
cdpCacheCapabilities.1.2 = 8
cdpCacheCapabilities.3.1 = 8
```

COMMAND DETAILS

object (p. 655)

object

- walkMIB *OBJECT*

```
The mib object to start from.
```

web-management

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show config (page 462)** **crypto (page 135)** **crypto host-cert (page 143)**

```
Usage: [no] web-management [management-url] URL
                           [support-url] URL
                           [<plaintext | ssl [<TCP-PORT>] >]

Description: Enable/disable the device web server.

Parameters:

    o management-url - Specify URL to load when the [?] button is clicked
             on the device's web interface.

    o support-url - Specify URL to load when the Support tab is clicked
             on the device's web interface.

    o plaintext - optional keyword indicating that the http server should
             be enabled with no security.  If no parameters are specified,
             'plaintext' is implied.

    o ssl - required keyword indicating that the http server should be
             enabled with Secure Sockets Layer support.
             Note: The 'ssl' and 'plaintext' variants of the command
             function independently of each other.  Enabling http+ssl does
             not automatically prevent the device from accepting plaintext
             connections; you must explicitly disable plaintext connections
             with the command 'no web-management plaintext'

    o TCP-PORT - optional - TCP port on which the https server should listen
             for connections.  If not specified, this defaults to port 443.
             This is configurable for ssl connections only; the plaintext
             server always listens on the well-known port 80.
```

COMMAND STRUCTURE

- [no] web-management **management-url** -- Specify URL for web interface [?] button. **(p. 657)**
  - **management-url** -- Specify URL for web interface [?] button. (ASCII-STR) **(p. 657)**
- [no] web-management **plaintext** -- Enable/disable the http server (insecure). **(p. 657)**
- [no] web-management **ssl** -- Enable/disable the https server (secure). **(p. 657)**
  - **ssl-port** -- TCP port on which https server should accept connections. (TCP/UDP-PORT) **(p. 657)**
- [no] web-management **support-url** -- Specify URL for web interface Support page. **(p. 657)**
  - **support-url** -- Specify URL for web interface Support page. (ASCII-STR) **(p. 657)**

EXAMPLES

Example: web-management

Re-enable insecure web browser access:

```
ProCurve(config)# web-management
```

COMMAND DETAILS

management-url (p. 657)	**ssl (p. 657)**	**support-url (p. 657)**
plaintext (p. 657)	**ssl-port (p. 657)**	

management-url

- [no] web-management management-url

  ```
  Specify URL for web interface [?] button.
  ```

  Next Available Option:

  - **management-url** -- Specify URL for web interface [?] button. (ASCII-STR) **(p. 657)**

- web-management management-url *MANAGEMENT-URL*

  ```
  Specify URL for web interface [?] button.
  ```

plaintext

- [no] web-management plaintext

  ```
  Enable/disable the http server (insecure).
  ```

ssl

- [no] web-management ssl

  ```
  Enable/disable the https server (secure).
  ```

  Next Available Option:

  - **ssl-port** -- TCP port on which https server should accept connections. (TCP/UDP-PORT) **(p. 657)**

ssl-port

- web-management ssl *TCP/UDP-PORT*

  ```
  TCP port on which https server should accept connections.
  ```

support-url

- [no] web-management support-url

  ```
  Specify URL for web interface Support page.
  ```

  Next Available Option:

  - **support-url** -- Specify URL for web interface Support page. (ASCII-STR) **(p. 657)**

- web-management support-url *SUPPORT-URL*

  ```
  Specify URL for web interface Support page.
  ```

wireless-services

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: wireless-services <SLOT-ID> [<reload|shutdown>]

Description: Configure parameters for the wireless-services module or
             change the module's state (reload or shutdown).

Parameters:

    o <SLOT-ID> - Configure parameters for the wireless-services module.

    o <SLOT-ID> reload - Reboot wireless-services module.

    o <SLOT-ID> shutdown - Shutdown (halt) the wireless-services module.
```

NOTES

Multiple Contexts

This command also is available in the manager context and the operator context.

COMMAND STRUCTURE

- wireless-services **wireless-services** -- Configure parameters for the wireless-services module or change the module's state (reload or shutdown) (SLOT-ID) **(p. 660)**
  - **config** -- (ASCII-STR) **(p. 659)**
  - **diagnostic-restart** -- Reboot wireless-services module into diagnostic partition. **(p. 659)**
  - **reload** -- Reboot wireless-services module. **(p. 659)**
  - **shutdown** -- Shutdown (halt) the wireless-services module. **(p. 660)**
  - **tech** -- Enter the configuration context for the wireless-services module. **(p. 660)**

COMMAND DETAILS

config (p. 659)	**reload (p. 659)**	**tech (p. 660)**
diagnostic-restart (p. 659)	**shutdown (p. 660)**	**wireless-services (p. 660)**

config

- wireless-services *SLOT-ID* config *CONFIG*

diagnostic-restart

- wireless-services *SLOT-ID* diagnostic-restart

```
Reboot wireless-services module into diagnostic partition.
```

reload

- wireless-services *SLOT-ID* reload

```
Reboot wireless-services module.
```

shutdown

- wireless-services *SLOT-ID* shutdown

```
Shutdown (halt) the wireless-services module.
```

tech

- wireless-services *SLOT-ID* tech

```
Enter the configuration context for the wireless-services module.
```

wireless-services

- wireless-services *SLOT-ID*

```
Usage: wireless-services <SLOT-ID> [<reload|shutdown>]

Description: Configure parameters for the wireless-services module or
             change the module's state (reload or shutdown).

Parameters:

    o <SLOT-ID> - Configure parameters for the wireless-services module.

    o <SLOT-ID> reload - Reboot wireless-services module.

    o <SLOT-ID> shutdown - Shutdown (halt) the wireless-services module.
```

Next Available Options:

- **diagnostic-restart** -- Reboot wireless-services module into diagnostic partition. **(p. 659)**
- **reload** -- Reboot wireless-services module. **(p. 659)**
- **shutdown** -- Shutdown (halt) the wireless-services module. **(p. 660)**
- **tech** -- Enter the configuration context for the wireless-services module. **(p. 660)**
- **config** -- (ASCII-STR) **(p. 659)**

wireless-services

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: wireless-services <SLOT-ID> <reload|shutdown>

Description: Display parameters for the wireless-services module or
             change the module's state (reload or shutdown).
```

NOTES

Multiple Contexts

This command also is available in the config context and the operator context.

COMMAND STRUCTURE

- wireless-services SLOT-ID **diagnostic-restart** -- Reboot wireless-services module into diagnostic partition. **(p. 661)**
- wireless-services SLOT-ID **reload** -- Reboot wireless-services module. **(p. 661)**
- wireless-services SLOT-ID **shutdown** -- Shutdown (halt) the wireless-services module. **(p. 661)**

COMMAND DETAILS

diagnostic-restart (p. 661)	**reload (p. 661)**	**shutdown (p. 661)**

diagnostic-restart

- wireless-services *SLOT-ID* diagnostic-restart

```
Reboot wireless-services module into diagnostic partition.
```

reload

- wireless-services *SLOT-ID* reload

```
Reboot wireless-services module.
```

shutdown

- wireless-services *SLOT-ID* shutdown

```
Shutdown (halt) the wireless-services module.
```

wireless-services

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: wireless-services SLOT-ID

Description: Display parameters for the wireless-services module.

Parameters:

    o <slotID> - Device slot identifier for the wireless-services module.
```

NOTES

Multiple Contexts

This command also is available in the config context and the manager context.

COMMAND STRUCTURE

- wireless-services **slot-id** -- Device slot identifier for the wireless-services module. (SLOT-ID) **(p. 662)**

COMMAND DETAILS

slot-id (p. 662)

slot-id

- wireless-services *SLOT-ID*

```
Device slot identifier for the wireless-services module.
```

write

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show config (page 462)**

```
Usage: write <memory|terminal>

Description: View or save the running configuration of the switch.

             write terminal - displays the running configuration of the
                              switch on the terminal
             write memory   - saves the running configuration of the
                              switch to flash. The saved configuration
                              becomes the boot-up configuration of the switch
                              the next time it is booted.
```

COMMAND STRUCTURE

- write **memory** -- Save the running configuration of the switch to flash. **(p. 663)**
- write **terminal** -- Display the running configuration of the switch on the terminal. **(p. 663)**

EXAMPLES

Example: write memory

Make a configuration change (in this example, create a static IP route) and save the change to the configuration file in flash memory:

```
ProCurve(config)# ip route 192.0.0.0 255.0.0.0 195.1.1.1
ProCurve(config)# write memory
```

COMMAND DETAILS

memory (p. 663)	**terminal (p. 663)**

memory

- write memory

```
Save the running configuration of the switch to flash.
```

terminal

- write terminal

```
Display the running configuration of the switch on the terminal.
```

ProCurve
Networking by HP

March 2008

Manual Part Number
5992-3063